国信智库·博士后丛书

国家社科基金项目结项成果

电子政务
信息资源共享与安全保障机制

吕欣 等 著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书从电子政务信息资源共享与安全保障机制的理论入手，分析了二者之间的关系；对国内外电子政务信息资源共享的安全保障机制进行了比较研究，给出了国外经验对我国电子政务信息资源共享安全保障机制建设的几点启发；对电子政务信息资源共享的影响因素进行了分析，总结出电子政务信息资源共享安全风险的成因；研究给出了我国电子政务信息资源共享的安全保障机制建设案例，通过案例总结出我国电子政务信息资源共享方面存在的一些问题；通过模型分析研究提出了电子政务信息资源共享的安全保障机制；给出了健全我国电子政务信息资源共享安全保障机制的对策建议。

图书在版编目（CIP）数据

电子政务信息资源共享与安全保障机制 / 吕欣等著. —北京：电子工业出版社，2017.1

ISBN 978-7-121-30167-4

Ⅰ. ①电… Ⅱ. ①吕… Ⅲ. ①电子政务－信息资源－资源共享－研究－中国 Ⅳ. ①D63-39

中国版本图书馆 CIP 数据核字（2016）第 252926 号

策划编辑：董亚峰
责任编辑：董亚峰
特约编辑：赵树刚　罗树利等
印　　刷：北京季蜂印刷厂
装　　订：北京季蜂印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：720×1000　1/16　印张：15　字数：264 千字
版　　次：2017 年 1 月第 1 版
印　　次：2017 年 1 月第 1 次印刷
定　　价：48.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件到 dbqq@phei.com.cn。

本书咨询联系方式：QQ3502629。

“国信智库·博士后丛书”简介

“国信智库·博士后丛书”是由国家信息中心博士后科研工作站组织出版的博士后研究成果。国家信息中心是国家发展和改革委员会直接领导下的，以开发信息资源、服务科学决策为使命的，集信息技术、研究、管理于一体的机构，是直接服务于国家重大战略研究与制定的重要智库。国家信息中心博士后科研工作站是原国家人事部 2003 年正式批准设立，在理论经济学、应用经济学、管理科学与工程、社会学、网络空间安全、战略学和心理学 7 个学科具有单独招收博士后研究人员资格的科研工作站。目前博士后指导教师有三十多人，为博士后开展跨学科、跨领域的重大问题研究提供了全方位的指导。

博士后工作站一直秉持“明确目标，突出特色，紧密围绕经济社会发展前沿问题”的建站思路，致力于经济建设和信息化发展领域的理论和应用研究、政府决策咨询的高层次人才培养，形成了有特色的博士后培养模式。自建站以来，在国家人力资源和社会保障部及全国博士后管理委员会的领导下，在国家发展和改革委员会人事司和各位博士后导师的指导支持下，累计招收博士后研究人员近 70 人，在国家经济建设和信息化发展中发挥了日益重要的作用。

博士后在站期间直接参与重大课题和决策咨询研究，形成了一系列有价值的研究成果。自建站以来，除每位博士后的出站报告外，博士后站同时承担着国家重大科技专项、社会科学基金、自然科学基金、部委委托研究项目等。博士后通过实地调研撰写的研究报告，多篇获得中央和国务院有关部门的肯定。

为促进博士后研究成果的转化应用，发挥研究成果的社会效应，现集中整理本站博士后的优秀研究成果，编辑出版“国信智库·博士后丛书”。我们提倡创新、严谨、原创性研究，收录的研究作品均为博士后站研究人员的研究报告或阶段性研究成果。我们热切期待，社会各界特别是政策制定人士和学术界的朋友，能够关心、支持本丛书，并不吝赐教，使我们的工作不断完善。

前　言

党的十八届三中全会提出，全面深化改革的总目标是完善和发展中国特色社会主义制度，推进国家治理体系和治理能力现代化。电子政务作为政府管理服务的重要手段，对深化行政体系改革、加快政府职能转变、推进政府治理模式创新、激发经济社会发展活力具有重要的作用和意义。2015 年 8 月，国务院印发的《促进大数据发展行动纲要》（国发〔2015〕50 号）进一步将加快政府数据开放共享、推动资源整合、提升治理能力作为当前的主要工作任务。政务信息资源共享已经成为推动部门间政务服务相互衔接、协同联动、打破信息孤岛的重要举措，是深化简政放权、放管结合、优化服务改革的重要内容。

我国在电子政务信息资源共享方面已经取得了一些成就，但随着信息网络的普及和公众、企业对政务信息资源需求的加强，我国的电子政务信息资源共享也存在一些问题，主要表现在三个方面。首先，当前政府信息孤岛式依然突出，各部门数据的横向和纵向审核比对机制不健全，部门间难以相互协调沟通，影响了数据的质量和决策效率。其次，政务信息资源的共享程度不高，各部门之间数据的统一汇聚和共享机制不健全，政府部门之间对于数据的整合和交流工作比较滞后。最后，由于标准不统一，政务信息资源共享平台缺失，使得大量的、有价值的政府数据处于散乱和沉睡状态，既降低了政府的工作效率，又严重影响了企业界、科学界的应用创新进程，难以满足大数据时代“大众创业，万众创新”的数据需求。

当前政务信息资源共享程度不高的主要原因表现在三个方面：一是政府部门不愿共享信息，主要表现在缺乏政务信息资源共享的机制和激励措施，造成政府部门在信息资源共享过程中缺乏积极性和主动性；二是政府部门不便共享信息，主要表现在缺乏政务信息资源共享平台和渠道，造成政府部门不知道如何去共享信息；三是政府部门不敢共享信息，主要表现在缺乏政务信息资源共享的安全保

障机制，使得政府部门在信息资源共享工作中担心数据安全和数据保密问题。如何保证电子政务信息资源在共享过程中的安全性，以及如何处理好共享和安全之间的关系，是本书的重点研究内容。

本书的章节安排如下：

第 1 章给出了研究电子政务信息资源共享与信息安全保障的背景和意义，归纳了国内外关于电子政务信息资源共享方面的文献。

第 2 章主要研究了电子政务信息资源共享的相关基础理论。首先研究了电子政务信息资源和信息安全保障的概念，然后从系统学、信息经济学和信息管理学等不同角度总结了电子政务信息资源共享的相关理论。

第 3 章对国内外电子政务信息资源共享的安全保障机制进行了比较研究。从加强领导和协调、完善政策法规环境、强化保障措施和掌握新技术的发展创新方向等角度入手，总结了美国、欧盟、俄罗斯、日本、韩国和加拿大等国的电子政务信息资源共享的安全保障机制；从顶层设计、法律法规、信息安全基础设施建设、电子政务网络和系统安全体系、信息安全技术产业和人才培养与安全意识等角度出发，对我国电子政务信息资源共享的安全保障机制进行了总结；同时给出了国外经验教训对我国电子政务信息资源共享安全保障机制建设的几点启示。

第 4 章主要对电子政务信息资源共享的影响因素及安全风险进行了分析。以对跨部门信息资源共享中收益与风险的感知为立足点，对电子政务信息资源共享中的障碍、安全风险及管理机制等内容进行了实证分析，探讨了影响电子政务信息资源共享的主要因素及其影响方式和程度。

第 5 章对电子政务信息资源共享安全保障机制建设的案例进行了研究。选取了江苏、江西两个省和省会城市广州为案例，对这三个省（市）的电子政务信息资源共享安全保障机制进行研究分析，归纳了我国地方电子政务信息资源共享安全保障机制建设的一些成功经验，也总结了目前存在的一些问题，旨在提炼出可在全国推广的普遍性对策。

第 6 章构建了我国电子政务信息资源共享的安全保障机制。分析了我国电子政务信息资源共享安全保障机制的理论基础和实践依据，构建了电子政务信息资

源共享的安全保障机制理论模型，从战略、管理和技术三个基础保障要素入手，结合当前我国电子政务信息资源共享中遇到的信息安全难点和关键问题，从宏观角度建立了我国电子政务信息资源共享的安全保障机制。

第 7 章研究了大数据的基本内涵及大数据对于电子政务的意义，分析了在大数据背景下电子政务的发展方向，给出了关于利用大数据推进电子政务信息资源共享和安全保障机制建设的几点思考。

第 8 章提出了健全我国电子政务信息资源共享安全保障机制的政策建议。以第 6 章的理论模型和保障机制研究为基础，围绕战略保障机制、管理保障机制和技术保障机制三个维度，提出了加强战略统筹、实施顶层设计、健全法律法规、完善管理体制、强化运行保障机制、推进新技术的应用和实施自主创新战略等建议。

本书为国家社科基金青年项目“电子政务信息资源共享的安全保障机制”（项目编号：07CTQ010）的研究成果。吕欣为项目负责人，项目组主要成员有：吕汉阳、杨月圆、郭艳卿、高枫、裴瑞敏、罗程等。项目研究过程得到了中国工程院何德全院士和国家信息中心有关领导的支持指导，李阳、王绍玉、刘瑾、白娇等同志对书稿的完善和校对做了大量的工作，在此表示衷心的感谢。感谢电子工业出版社的董亚峰在本书出版过程中给予的大力支持。

目　录

第 1 章　绪　论

1.1　选题背景和意义

电子政务信息资源（E-Government Information Resources）是政府部门在履行国家行政事务管理职能过程中产生的各种电子化的政府信息资源，包括一个国家在政治、经济、文化、社会等多方面的信息，是政府行政管理工作的基础和科学决策的依据。在落实科学发展观、建设节约型社会、推动政府职能转变、促进经济社会全面发展的要求下，电子政务信息资源共享作为合理配置资源、强化综合监管、完善宏观调控的有效手段，已经成为政府进行社会管理和宏观决策的重要支持，成为推进电子政务取得实质性进展的关键所在。

近年来，我国积极开展电子政务信息资源共享基础设施建设，已经取得了令人瞩目的成果。2015 年，地市、区县和乡级网络接入工作继续推进且覆盖面日益扩大。截至 2015 年年底，已接入政务外网的市（地、州、盟）和县（市、区、

旗）总数分别达到 314 个和 2493 个，其中地市级和区县级覆盖率分别达到 94.3%和 87.4%，计入新疆生产建设兵团，则地市级和区县级政务外网整体覆盖率分别达到 94.6%和 88%。重庆市和宁夏回族自治区于 2015 年实现了市、区级政务外网全覆盖，使全国实现市、区级政务外网全覆盖省份数量达到 25 个；北京、天津、上海、湖南、贵州等 16 个省（自治区、直辖市）网络向乡镇延伸，为进一步打通政府政务外网纵向服务渠道、向乡镇级各政务部门提供服务创造条件，政务外网乡级覆盖率达到 34.4%。政务外网已成为我国覆盖面最广、连接政务部门最多、承载业务类型最丰富的政务公用网络平台。国家人口基础信息库、法人单位基础信息库、自然资源和空间地理基础信息库、宏观经济数据库的建设取得了重要进展。以“十二金”为基础的涉及国计民生的国家“金字工程”和重大项目获得了良好的社会效益。在电子政务信息资源共享方面，北京、广东、南京、深圳等省市出台了针对电子政务信息资源共享的管理办法，长三角、珠三角、环渤海等地区在区域电子政务互联互通、信息资源共享工作上也进行了有益的探索。

然而，我国电子政务建设中条块分割的现状仍未得到有效解决，政务信息资源共享“纵强横弱”的局面未有根本改善，系统间互联互通遭遇重重阻碍，跨部门信息资源共享和业务协同推进迟缓。有关部门调研了 38 个中央部委，发现存在 80 个专网，且专网间实现横向交互的比例很低。电子政务信息资源共享在实际推行过程中长期面临一些阻碍，使得电子政务建设的经济社会效益未得到充分发挥，制约了政府的社会管理能力和公共服务水平，制约了法治政府、服务政府、效能政府的建设进展。电子政务信息资源共享受阻，其中一个重要原因就是：在电子政务信息资源共享过程中，随时可能面临各种各样的威胁，如电脑故障、病毒感染，以及遭遇黑客的入侵、泄密、篡改、个人隐私泄露等。据 Gemalto 公司报告数据显示，2015 年全球各地共发生 1673 起数据泄密事故，涉及 7.07 亿条数据记录。360 公司的补天漏洞预警平台显示，我国数据泄露问题日益严峻，2011—2014 年共发生重大数据泄露事件 100 起，导致 11.1 亿条数据泄露，其中在 21 次重大数据泄露事件中，每次涉及用户规模都在 1000 万人以上。据国家互联网应急协调处理中心监测，我国约 60%的部委级网站存在不同程度的安全隐患，如果发生政务信息泄露或被不正当利用，则会对国家安全、社会稳定、国家财产构成严重威胁。电子政务信息资源事关国家政治安全、经济安全、国防安全和社会稳定，如果被泄露或被不正当利用，则会对国家安全、公民隐私、单位财产构成严重威胁。

近年来，我国电子政务信息安全基础设施建设成效显著，信息安全技术水平不断提高，信息安全研发和产业化持续推进，电子政务整体抗风险能力逐渐增强。但是，由于我们对电子政务信息资源共享的安全风险缺乏科学认识，对电子政务信息资源共享和安全的相互作用机理缺乏深入理解，未能有效把握机制建设对于电子政务信息资源共享安全保障工作的关键作用，使得有关部门对信息资源共享过程中可能产生的不良后果和需承担的责任多有顾忌，信息安全问题成为制约电子政务信息资源共享工作深入推进的重要瓶颈。

电子政务信息资源共享面临怎样的安全风险？这些安全风险与电子政务信息资源共享的作用机理是怎样的？如何构建电子政务信息资源共享的安全保障机制？如何在保障信息安全的前提下充分有效地进行电子政务信息资源共享？这些问题都需要认真思考和深入研究。本研究旨在从理论和实证研究方面剖析共享和安全的相互作用机理，分析政府信息资源共享的安全风险，研究总结可在我国广泛推广的普遍性经验，服务于我国电子政务信息资源共享的安全保障机制建设，为推动国家信息化和信息安全协调发展，提高我国电子政务信息资源共享程度和利用水平提供理论和政策依据。

1.2　国内外研究现状

信息资源共享和信息安全一直是电子政务建设的两项核心工作，也是近年来电子政务实践工作的瓶颈，得到国内外学术界与实践界的广泛关注。

1.2.1　国内外相关文献检索

以“电子政务”为题名关键词在维普资讯网上进行检索，结果显示，“电子政务”名词 1999 年第一次出现在文献中；在 1999—2001 年，相关文献较少；自 2002 年开始，“电子政务”开始得到广泛的探讨，并在 2004—2005 年文献达到顶峰。1999—2014 年，以“电子政务”为题名关键词的文献共有 40 264 条（检索时间：2014 年 9 月 9 日），呈现 Gompertz 增长趋势（见图 1-1），这说明国内关于电子政

务的研究已经进入快速增长阶段，在研究方式上表现为从单纯对电子政务相关问题作定性分析到越来越多的人开始深入研究电子政务的某个热点问题，其中对电子政务信息资源共享和信息安全问题的探讨逐年增多；目前电子政务的研究还表现出研究问题比较集中、瓶颈问题尚未得到根本解决、工程研究多、机制问题研究少等特点。

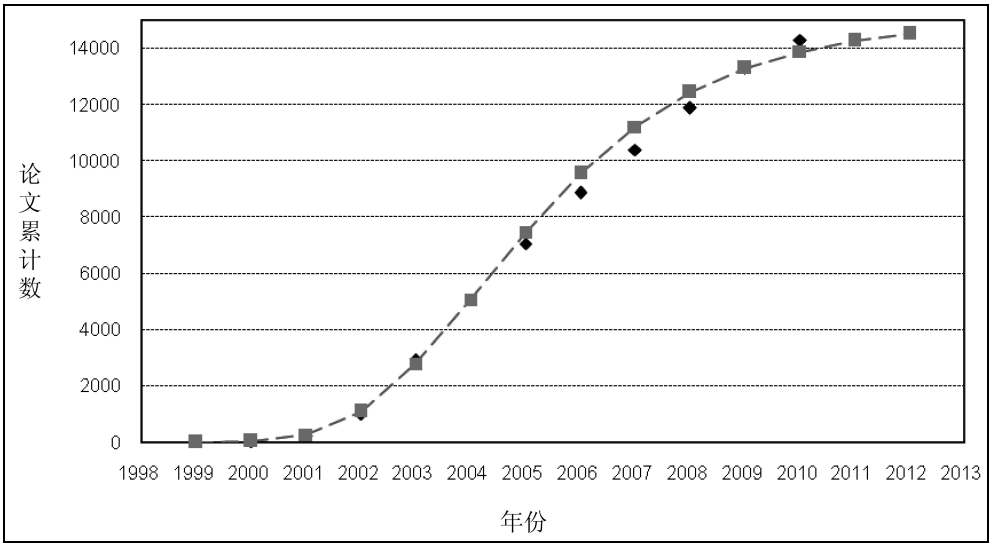


图 1-1　国内“电子政务”文献的 Gompertz 增长模型（拟合度：0.98）

以“电子政务信息资源”为检索词，自 2002 年开始有第一篇之后，到目前为止，文献总数为 1655 篇（检索日期：2014 年 9 月 9 日）；用“电子政务”和“信息资源”为题名对之进行模糊匹配检索时，可检索到文献 2091 篇（2001—2014.9.9）；进一步检索“电子政务信息资源共享”的相关文献，可以检索到文献 844 篇（2004—2014 年），模糊匹配检索 149 条，而单独与“信息资源共享”相关的文献却多达 7487 篇（2004—2014 年）。可见，我国将电子政务与信息资源（共享）相结合的研究在数量上还不是很多，但已经引起学术界的关注。

在信息安全方面，与“电子政务信息安全”相关的文献有 1477 篇（1992—2014 年），将“电子政务”与“信息安全”进行模糊匹配搜索也仅有 1762 篇（1992—2014 年），而单独与“信息安全”相关的文献多达 73 778 篇（1992—2014 年）。

尽管我国对电子政务、信息资源（共享）和信息安全的研究相对较多，范围也较为广泛，成果显著，但将电子政务与信息资源（共享）或信息安全相结合的研究却较少，而将三者结合，探索其相互关系和保障机制的研究更是少之又少。

关于国外的相关研究，对 Academic Search Premier（学术期刊数据库，ASP）、ProQuest Digital Dissertations（学位论文数据库，PQDD）等相关数据库进行了全面细致的检索，其文献来自欧美地区 1000 多所高等院校。同时，对 Web of Science 的 SCI expanded、SSCI、CPCI-S 和 CPCI-SSH 数据库以“E-Government”为检索词在“Topic”中进行了检索，发现第一次出现“E-Government”的文献是在 1999 年，研究论文逐年增长，并且会议论文占 74%左右，说明国外关于电子政务方面的研究也始于 20 世纪末和 21 世纪初。到目前为止，会议论文占绝大多数的现象说明了电子政务相关研究已经成为政府和学术界国际学术会议的研究话题，如图 1-2 所示。

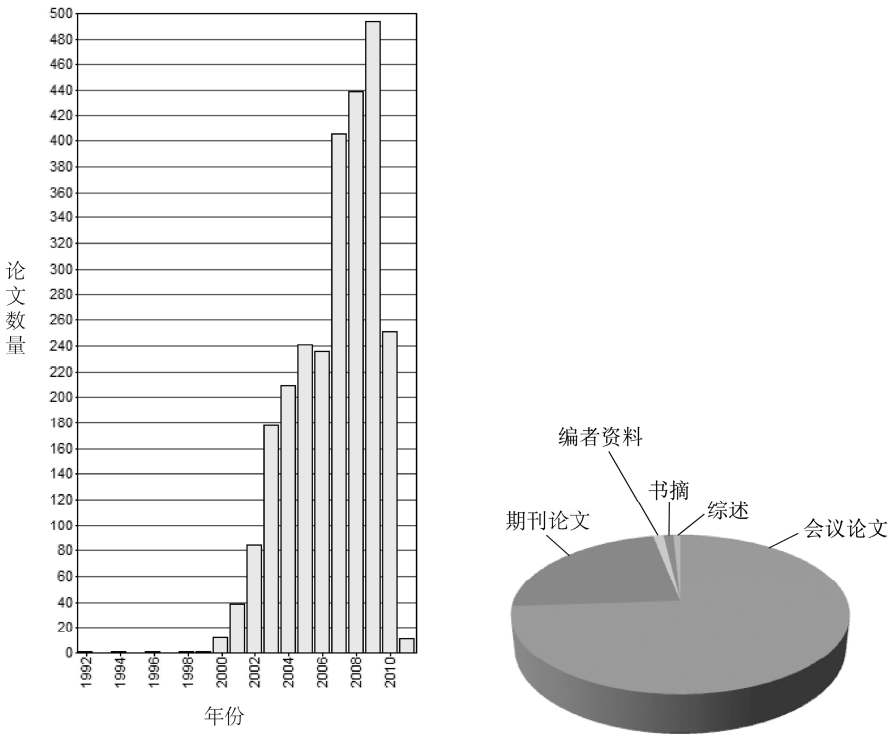


图 1-2　WoS“电子政务”文献分布情况

检索结果发现，国内外对信息资源共享问题的研究大都是从电子政务研究开始的，起步比较早，取得的研究成果相当丰富，但关于电子政务信息资源共享和信息安全之间关系及保障机制的研究却较少涉及。

1.2.2 国内外文献综述

1. 电子政务信息资源共享相关研究

电子政务信息资源共享是指通过跨部门、跨地区信息系统互联互通，对政府信息资源进行重新组合和优化配置，以实现公共服务和管理的政策目标。党的十八大报告明确提出，“创新行政管理方式，提高政府公信力和执行力”，电子政务作为政府工作的重要载体，发挥着关键作用。美国图书馆学家 Kent 认为，“资源共享”最确切的意义是指互惠，开展资源共享的唯一途径是拥有可供共享的资源、具有共享资源的意愿和实施资源共享的计划[1]。国外学者对信息资源共享的研究一直伴随着信息资源共享实践的发展而发展，总的来说，主要集中在两个方面：电子政务信息资源共享的制约因素和共享机制。

（1）电子政务信息资源共享的制约因素研究

电子政务信息资源共享的发展经历了三个阶段：单个机构之间的信息资源共享；建立信息资源共享平台；整合法律、管理和政策等方面来达到协同共享[2]。Landsbergen 等将技术因素引入跨组织的信息资源共享中，提出一个以技术、协同性和制度为核心的联邦政府-州政府间协同业务支持架构。

Dawes 在分析信息资源共享中存在的技术、组织和政治上三种类型的障碍、风险和收益的基础上，提出了部门间信息资源共享的理论模型，并提出两个信息资源共享的政策原则——管理工作和有用性，认为这些因素可以促进信息资源共

[1] Allen Kent. The Goals of Resource Sharing in Libraries[C]. Proceeding of the 1976 Conference on Resource Sharing in Libraries. Pittsburgh, Pennsylvania, 1977: 17-18.

[2] L David，W George . Government Information Systems and the Fourth Generation of Information Technology [J]. Public Administration Review, 2001, Vol. 61(2): 206-220.

享过程中的收益，减少信息资源共享过程中的风险[3]。Anitesh Barua 等分析了组织、技术等因素对信息资源共享的影响，提出再造组织中的信息资源共享行为，创建一个可以促进信息有效共享的环境[4]。Kolekofski 和 Heminger 研究了一定组织背景下影响信息资源共享目的的信念因素[5]。Akbulut 从实证的角度对影响美国州政府和地方政府部门之间电子信息资源共享的因素进行了研究[6]。2004 年，David 等人通过研究指出不同文化环境中的成员之间的误解和不信任是信息资源共享的最大障碍[7]。Lee 和 Kim 研究了影响电子政务的知识共享能力的三个因素：组织文化、组织结构和信息技术，认为这三个因素是相互独立的组织维度变量[8]。Evgeniou 等分析了影响组织信息智能水平的行为障碍、过程障碍和组织障碍[9]。Shin 等研究了社会文化因素对信息资源共享的影响[10]。

还有研究认为信息资源共享中的期望收益是人们进行信息资源共享的重要因素之一，而人们感知到的可能存在的风险是信息资源共享最大的阻力，并且人们关于信息资源共享的预期收益和风险受到管理、文化、IT 技术、政策等方面的影

[3] Dawes, S. S. Interagency information sharing: Expected benefits，manageable risks[J] . Journal of Policy Analysis and Management, 1996, Vol. 15(3), 377-394.

[4] Barua A., Ravindran S. Reengineering Information Sharing Behavior in Organization[J]. Journal of Information Technology, 1996, Vol. 11(3): 261-272.

[5] Kolekofski Jr, K. E., Heminger, A. R. Beliefs and Attitudes Affecting Intentions to Share Information in an Organizational Setting[J]. Information＆Management, 2003, Vol. 40(6): 521-532.

[6] Akbulut, A. Y. An Investigation of the Factors that Influence Electronic Information Sharing Between State and Local Agencies[D]. Louisiana State University, 2003.

[7] Drake, D. B., Steekler, N. A., Koch, M. J. Information Sharing in and Across Government Agencies: The Role and Influence of Scientist, Politician and Bureaucrat Subcultures[J]. Social Science Computer Review, 2004, Vol.22(1): 67-84.

[8] Lee, H., Kim, S. Organizational Factors Affecting Knowledge Sharing Capabilities in E-Government:an Empirical Study[J]. National Conference on Digital Government Research, 2004, Vol.3035: 281-293.

[9] Evgeniou, T., Cartwright, P. Barriers to Information Management[J]. European Management Journal, 2005, Vol. 23(3): 293-299.

[10] Shin, S.K., Ishman, M., Sanders, G. L. An Empirical Investigation of Socio-Cultural Factors of Information Sharing in China[J]. Information & Management, 2007, Vol. 44(2): 165-174.

响[11]。同时，一些文化因素也得到了关注，Shin 认为中国的一些传统文化，例如关系、儒家文化和集体主义感可以解释中国人之间的信息资源共享过程[12]。Yan Zhijun 等基于 DeLone&McLean 模型研究了电子政务信息资源共享的影响因素，提出信息质量、信息使用、感知收益、信任、感知可用性、感知易用性这些因素影响用户共享信息的意向[13]。

Roberts 经过大量系统的研究，指出在遭受“9·11”恐怖袭击以后，美国本土的安全形势每况愈下，其主要原因就是信息资源共享没有得到足够的重视，美国政府部门之间收集和发布有关遭遇袭击的准确信息的程序相当不健全，有关责任部门难以获得关于袭击的可靠信息。他认为，各职能部门间信息资源共享和沟通机制的不健全是难以有效发现和阻止各种袭击发生的主要原因[14]。虽然美国出于国土安全等战略的考虑对信息资源共享日益重视，但在新的反恐网络内部推动信息资源共享依然存在着诸多障碍：一是宪法的某些约束；二是一些技术上的障碍，如联邦政府机构的通信和信息系统的兼容性和互操作性的不足；三是官僚体制和文化方面的障碍，如组织间的不信任，认为信息资源共享之后，一个机构的某个项目会承担风险。Relyea 同样认可信息资源共享没有得到足够的重视是造成“9·11”恐怖袭击的影响因素之一，从联邦政策出发研究了信息资源共享的程序[15]。

Bekkers 通过研究荷兰电子政务协作管理提出，电子政务建设需要制定灵活的

[11] Gil-Garcia, J. R., Chengalur-Smith, I., Duchessi, P. Collaborative e-Government: Impediments and Benefits of Information-sharing Projects in the Public Sector[J]. European Journal of Information Systems, 2007, Vol. 16(2): 121-133.

[12] Shin, S. K., Ishman, M., Sanders, G. L. An Empirical Investigation of Socio-cultural Factors of Information Sharing in China[J]. Information & Management, 2007, Vol. 44(2): 165-174.

[13] Yan Zhijun, Baowen Sun, Tianmei Wang. A Study on Information Sharing of E-Government[C]. Proceedings of 2009 IEEE International Conference on Grey Systems and Intelligent Services, 2009:1331-1335.

[14] Roberts, A. S., & Governance, N. Networked Governance, Information Sharing and the Threat to Government Accountability[J]. Government Information Quarterly, 2004, Vol. 21(3): 249-267.

[15] Relyea, H. C. Homeland security and information sharing: Federal policy considerations[J]. Government Information Quarterly, 2004, Vol. 21(4): 420-438.

信息架构，不仅要考虑技术方面的因素，同时也不能忽视政治、经济、法律等政策的协作[16]。Gonzalo Valdés 等探讨了开发和实施电子政务的成熟度模型[17]。Liu Wenjing 从国家视角研究了电子政务信息资源共享的原则、实践和问题，分析对比了美国、英国、挪威、巴西和中国的电子政务信息资源共享实践，提出在电子政务信息资源共享中应综合考虑合法和合理、司法公正、隐私权保护、权利分割和纠纷处理五方面因素，遵循合法性、必要性、合理性、透明性、灵活性等基本原则[18]。Yang 和 Maxwell 将信息资源共享的影响因素分为人与人之间、组织内部间和组织外部间三个层面，提出法律和政策、组织机构、不同的操作程序和工作流、组织间的信任、对信息误用等影响着组织间的信息资源共享水平[19]。Ardion Beldad 等通过来自荷兰三个城市的 208 份网络用户的测试情况，研究表明在电子政务中用户个人隐私信息披露的意愿与用户对政府的信任正相关而与可预知的风险负相关[20]。

此外，随着信息技术的发展，一些学者研究了新技术为信息资源共享带来的新机遇。如 Rosenthal 等研究了云计算在生物信息资源共享领域的应用[21]；Tsui

[16] Bekkers, V. Flexible Information Infrastructures in Dutch E-Government Collaboration Arrangements: Experiences and Policy Implications[J]. Government Information Quarterly, 2009, Vol. 26(1): 60-68.

[17] Valdés, G., Solar, M., Astudillo, H., et al. Conception Development and Implementation of an E-Government Maturity Model in Public Agencies[J]. Government Information Quarterly, 2011, Vol. 28(2): 176-187.

[18] Liu Wenjing, Government information sharing: Principles, practice, and problems--An international perspective[J]. Government Information Quarterly, 2011, Vol.28(3): 363-373.

[19] Yang, T., Maxwell, T. A. Information-Sharing in Public Organizations: A Literature Review of Interpersonal Intra-Organizational and Inter-Organizational Success Factors[J]. Government Information Quarterly, 2011, Vol. 28(2):164-175.

[20] Beldad, A., Jong, M.D., steehouder, M. I Trust not Therefore it Must be Risky: Determinants of the Perceived Risks of Disclosing Personal Data for E-Government Transactions[J]. Computers in Human Behavior, 2011, Vol. 27(6):2233-2242.

[21] Rosenthal, A., Mork, P., Li, M.H, et al. Cloud Computing: A New Business Paradigm for Biomedical Information Sharing[J]. Journal of Biomedical Information, 2010, Vol. 43(2): 342-353.

等、Freeman 和 Loo 分别探讨了 Web 2.0 给电子政务带来的机遇[22,23]；Li Zhitao 等探讨了云计算在高性能计算、信息资源共享等方面为电子政务带来的便利[24]；杨传明做了 Web 2.0 环境下政府网站数字信息资源共享服务实证研究[25]；陈敏克等研究了基于云计算的农业信息资源共享系统建设[26]。

（2）电子政务信息资源共享机制相关研究

关于电子政务信息资源共享机制的研究，影响较大的是 Akhilesh 和 Sudha 2003 年提出的“机构互联信息资源共享（IAIS）”模型[27]。IAIS 是基于 XML 标准的一种信息资源共享模型。过去人们主要关注于结构化数据的整合和共享，现在开始关注于非结构化数据的整合和共享。信息资源共享首先要求各部门间联合制定良好的、统一的规划，规划可避免各种不同数据库之间的错误、语意冲突、关系冲突以及属性值的不一致。IAIS 可以方便地定义需要共享的信息结构，也使得信息维护变得容易，检索也更为方便。Kwon 等探讨了政府信息资源数字化保护的机遇和挑战，提出通过开发国家政务数字化信息保护社区来促进政府部门跨组织之间的协作[28]。Gottschalk 探讨了电子政务中的互操作问题，提出了一个包括计算机互操作性、处理互操作性、知识互操作性、价值互操作性和目标互操作性在内的五层模型[29]。Jiang Dingfu 等研究了电子政务中社会化信息的协作共享模

[22] Hau-Dong Tsui, Chong-Yen Lee and Ching-Bang Yao. Creating a Web 2.0 Government: Views and Perspectives. 2nd International Conference on Networking and Digital Society, 2010: 648-651.

[23] Raoul J. Freeman, Peter Loo. Web 2.0 and E-Government at the Municipal Level. 2009 World Congress on Privacy, Security and Trust and the Management of e-Business, 2009:70-78.

[24] Li Zhitao et al., Study of the seismic system E-Government based on Cloud Computing. 2010 International Conference on E-Business and E-Government, 2010:2129-2132.

[25] 杨传明．Web 2.0 环境下政府网站数字信息资源共享服务实证研究[J]．图书馆情报工作，2011（9）：126-129.

[26] 陈敏克等．基于云计算的农业信息资源共享系统建设研究[J]．农业网络信息，2011（4）.

[27] Akhilesh, B., & Sudha. IAIS: A Methodology to Enable Interagency Information sharing in E-Government[J]. Journal of Database Management, 2003, Vol. 14(4):59-80.

[28] Kwon, H., Pardo, T. A., Burke, G. B. Interorganizational Collaboration and Community Building for the Preservation of State Government Digital Information: Lessons from NDIIPP State Partnership Initiative[J]. Government Information Quarterly, 2009, Vol. 26(1):186-192.

[29] Gottschalk, P. Maturity Levels for Interoperability in Digital Government[J]. Government Information Quarterly, 2009, Vol. 26(1):75-81.

型，分别提出了政府组织间、政府内部以及纯公共信息的共享模型。研究认为，协作模型能够提高服务、优化信息资源、实现跨区域信息资源共享的长期双赢发展[30]。Celene Navarrete 等提出了一种整合信息资源共享多种影响因素框架，用于实现跨国电子政务信息资源共享、协作和互操作[31]。Li Liming 等和 Ye Xin 等分别从技术角度提出了电子政务信息资源整合框架[32,33]。熊曙初和罗毅辉提出了以协同域为基本单位，以协作成员、协作任务等为要素的政务协同服务过程模型，模型能实现电子政务协同服务链动态构建，提高电子政务群体协同服务的质量和效率[34]。胡海波从战略的视角探讨了政务信息流程重组的规划目标、架构和层次，提出了政务信息流程重组的优化路径，以及实现政务协同和政务管理变革的思路[35]。陈勇跃和夏火松就当前我国政府部门间的信息资源共享水平低、存在诸多障碍因素的现状进行了分析，研究了跨政府部门信息资源标准化建设的问题[36]。蒋明敏和赵春雷就网络环境下政府信息资源共享的基本模式与制度保障进行了研究，认为消解政府信息资源共享的障碍，关键是确立并执行一套适合中国国情的信息管理制度[37]。

---

[30] Jiang Dingfu, Xiong Li, Xiang Zhengtao. Collaborative Sharing Model of Socialized Information in Yangtze River Delta Region[C]. 2010 International Conference on Management of e-Commerce and e-Government 2010, 2010:244-247.

[31] Celene Navarrete, et al. Multinational E-Government Collaboration, Information Sharing and Interoperability: An Integrative Model[C]. Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010:1-10.

[32] Li Liming, et al. The Information Resource Integration in E-government Based on EAI[C]. 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2010:21-24.

[33] Ye Xin, et al. The inter-organizational business collaboration oriented role model for E-government [C]. 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2010:45-48.

[34] 熊曙初，罗毅辉．基于协同体的电子政务协同服务元模型研究[J]．情报杂志，2010（9）：162-166．

[35] 胡海波．基于战略的政务信息流程重组研究[J]．电子政务，2011（4）：46-52.

[36] 陈勇跃，夏火松．跨部门政府信息资源共享标准构建研究[J]．情报理论与实践，2010（12）：25-28．

[37] 蒋明敏，赵春雷．网络环境下政府信息资源共享的基本模式与制度保障[J]．河南社会科学，2011（1）：77-80．

2．电子政务信息安全相关研究

美国军方将信息安全（INFOSEC）定义为：保护和预防信息和信息系统被非授权访问，以及对信息的篡改，同时要保护系统不拒绝用户正常使用。信息安全包括通信保密（COMSEC）和计算机安全（COMPUSEC）等研究内容。BS7799把信息安全定义为：保证信息的保密性、完整性和可用性。保密性就是保证信息仅被授权的人所访问；完整性是指保护信息和处理方法的精确性与完整性；可用性是指保证授权用户在需要时可以访问信息和相关资产。同时，把信息安全看作执行一组可以是策略、实践、过程、组织结构和软件功能等的控制，通过建立这些控制以保证组织的安全目标得以实现。欧共体把信息安全定义为：在既定的密级条件下，网络与信息系统抵御意外事件或恶意行为的能力。这些事件和行为将会危及所存储和传输的数据以及由这些网络和系统所提供服务的可用性、真实性和保密性。在信息社会，信息安全的概念已经不再局限于信息和信息系统等物理实体，它已渗透到生产、生活、工作和娱乐等的各个方面。对于电子政务网络系统来说，政务信息事关国家政治安全、经济安全、国防安全和社会稳定，如果政务信息被泄露或被不正当利用，将会对国家安全、公众隐私、单位财产构成严重威胁，后果不堪设想。因此，电子政务信息安全问题研究得到了国内外学者的高度重视。

McMillen 通过实证研究从隐私保护、数据机密性角度分析了数据共享的安全问题[38]。Sarathy 和 Muralidhar 从技术角度研究了数据共享的安全问题[39]。Zissish 和 Lekkas 研究了开放云计算架构下的安全电子政务在线投票方案[40]。Belanger 和 Carter 研究了电子政务中信任和风险之间的关系[41]。Li Jianxin 等研究了开发计算环境中跨域资源共享和协作的安全问题，提出了一个安全协作服务来实现动态虚

[38] McMillen, D. Privacy, Confidentiality, and Data Sharing: Issues and Distinctions[J]. Government Information Quarterly, 2004, Vol. 21(3):359-382.

[39] Sarathy, R., Muralidhar, K. Secure and Useful Data Sharing[J]. Decision Support Systems, 2006, Vol. 42(1):204-220.

[40] Zissis, D., Lekkas, D. Securing E-Government and E-Voting with an Open Cloud Computing Architecture[J]. Government Information Quarterly, 2011, Vol. 28(2):239-251.

[41] Belanger, F. Carter, L. Trust and Risk in E-Government Adoption[J]. Journal of Strategic Information Systems, 2008, Vol. 17(2):165-176.

拟组织的管理，并设计了相关协议[42]。Jensen 和 Zhao 对美国电子政务网站进行了包括网站内容分析、信息安全审计和计算机网络安全等在内的安全评估，讨论了电子政务安全的威胁和挑战，并给出了相关解决方案[43]。Lai 等通过实证研究分析了信任在基于互联网的跨组织的系统中的影响，并提出了一个信任模型[44]。Liu Yan 和 Zhou Changfeng 提出了一个电子政务服务的公民信任模型，分析认为感知可用性、感知风险、感知安全等是影响公民对电子政务信任的重要因素[45]。Bruno 和 Valipuram 提出了一种用于电子政务之中用户可以自主选择隐私等级和安全需求的概念模型[46]。Dinara 等提出了一个可信平台模块来解决电子政务中的电子税收安全问题[47]。Wang Shaohui 和 Sun Yunchong 从管理、技术、法律三个角度分析了电子政务信息安全风险，并在此基础上提出了电子政务信息安全保障系统的框架[48]。

曲成义研究了内、外网信息安全面临的挑战及对策，研究了电子政务信息安全体系框架[49,50]。吕欣在其博士后研究报告中从系统学的角度分析了电子政务信

[42] Li Jianxin et al.. A secure collaboration service for dynamic virtual organizations[J]. Information Sciences, 2010, Vol. 180(17): 3086-3107.

[43] Zhao, J. J., Zhao, S. Y. Opportunities and Threats: A Security Assessment of State E-Government Websites[J]. Government Information Quarterly, 2010, Vol. 27(1): 49-56.

[44] Lai, I. K. W., Tong, V. W. L., Lai, D. C. F. Trust Factors Influencing the Adoption of Internet-Based Interorganizational systems[J]. Electronic Commerce Research and Application, 2011, Vol. 10(1): 85-93.

[45] Yan Liu, Changfeng Zhou. A Citizen Trust Model for E-government[C].2010 IEEE International Conference on Software Engineering and Service Sciences, 2010:751-754.

[46] Bruno Lage Srur and Valipuram Muthukumarasamy. Enhancing Trust on e-Government: A Decision Fusion Module[C]. 2009 Third International Conference on Network and System Security, 2009: 164-169.

[47] Dinara Berdykhanova, Ali Dehghantanha and Kumaresh Hariraj. Trust Challenges and Issues of E-Govemment: E-Tax Prospective[C]. 2010 International Symposium inInformation Technology, 2010:1015-1019.

[48] Wang Shaohui and Sun Yunchong. Research on Information Security Assurance System of E-government[C]. International Conference onComputational Intelligence and Software Engineering, 2009:1-4.

[49] 曲成义．内网信息安全面临的挑战及对策[J]．信息网络安全，2008（5）：7-8.

[50] 曲成义．电子政务信息安全保障体系探讨[J]．信息技术与标准化，2003（11）：19-23.

息空间的演化行为，深入研究了电子政务信息空间及其安全保障体系的复杂巨系统特征，建立了电子政务信息安全保障理论模型，从宏观上提出了电子政务信息安全保障策略。何振和周伟从网络安全、信息保密、网络信息侵权、信息资源污染等方面研究了信息安全给政务信息资源共享带来的影响，并提出了有关对策[51]。范静研究了电子政务中信息资源共享的信息安全影响因素，对各个因素与共享绩效之间的关系进行了检验，首先对不同因素进行因子分析，提取高层次的因子，然后研究高层次的因子与共享绩效之间的关系[52]。

综上分析，国内外学者在电子政务信息资源共享和信息安全等方面进行了大量的研究，从电子政务信息资源共享的制约因素到共享机制和安全体系等方面均有讨论。但是电子政务信息资源共享的信息安全问题研究较少，特别是缺乏对政务信息安全和共享的相互作用和制约关系方面的研究，缺乏从整体上对电子政务信息资源共享的安全保障机制建设的研究工作。

1.3 研究思路和方法

1.3.1 研究思路

本研究有机结合了系统科学和信息科学方法，综合运用系统学、信息经济学、信息管理学等理论与方法，将理论分析与实证研究紧密结合，采用文献调研、问卷调查、实地调研、专题研讨、专家访谈等方法，结合理论模型与实证分析，从理论探索电子政务信息资源共享与安全的相互作用机理入手，结合国内外电子政务信息资源共享安全保障机制的建设状况，分析了电子政务信息资源共享面临的安全风险，构建了电子政务信息资源共享的安全保障机制模型并加以解析，进而提出加强我国电子政务信息资源共享安全保障的实现机制和策略。

[51] 何振，周伟. 电子政务信息资源共建共享的信息安全问题分析[J]. 档案时空，2005（4）：8-10.
[52] 范静．G2G 电子政务信息资源共享及信息安全实证研究[D]．上海交通大学，2008.

本研究按照研究对象界定、研究方法确定、理论研究、实证研究、模型构建、对策建议设计的思路展开，如图 1-3 所示。

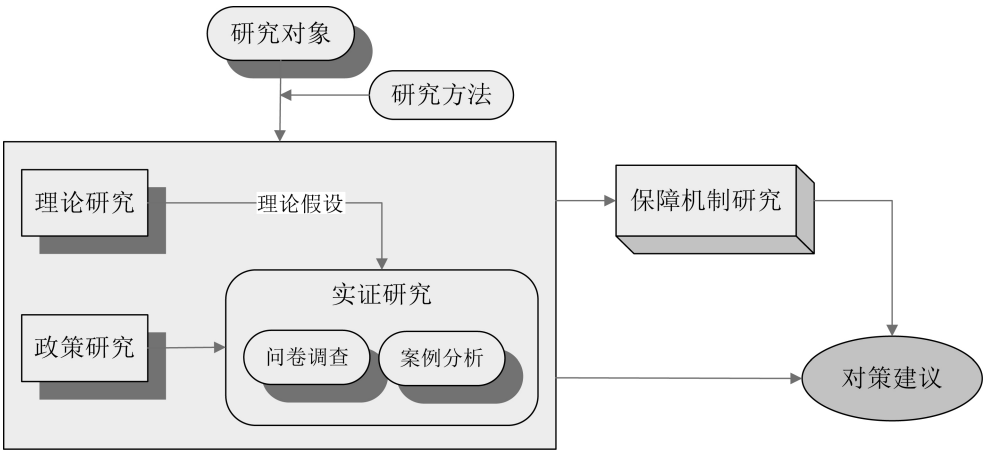


图 1-3　技术路线

1.3.2　研究方法

1．自然科学与社会科学相结合的研究方法

采用系统学、管理学、信息经济学等学科相结合的综合集成法对电子政务信息资源共享的安全机制进行分析和研究。

2．理论研究与实践研究相结合的研究方法

在理论方面，研究了电子政务信息资源共享理论、电子政务信息安全保障理论以及电子政务信息资源共享安全保障机制，并分别从系统学、管理学和信息经济学角度研究和分析了电子政务信息资源共享与信息安全保障之间的关系；在实践方面，以理论研究为基础，进行了电子政务信息资源共享的案例研究和影响因素及安全风险分析的实证研究。

3．定性研究与定量研究相结合的研究方法

在定性研究方面，研究了电子政务信息资源共享的信息安全保障相关的理论

并提出了相应的安全保障机制，分析了电子政务信息资源共享的影响因素和安全风险，通过案例研究分析归纳出了电子政务信息资源共享的安全保障机制建设的成功经验；在定量研究方面，通过问卷调查的方法对电子政务信息资源共享的影响因素和安全风险进行回归分析，定量研究影响因素的重要程度和安全风险的大小。

1.4 研究内容

“电子政务信息资源共享的安全保障机制”是一个涉及情报学、信息科学、系统科学、管理科学等多个学科的研究领域，同时也是与国民经济、社会稳定和国家安全结合非常紧密的研究课题。本研究主要关注政府间的电子政务（G-G），在信息资源共享中，着重研究跨部门的信息资源共享。

本项目从以下六个方面开展研究，对我国电子政务信息资源共享的安全保障机制建设提供理论依据和对策建议。

1．电子政务信息资源共享与安全保障理论研究

研究和归纳了电子政务信息资源共享与信息安全保障相关理论，主要包括电子政务信息资源共享理论、电子政务信息安全保障理论。从系统学、信息经济学和管理学等角度对电子政务信息资源共享与信息安全的相互作用关系进行了分析。

2．国内外电子政务信息资源共享的安全保障机制比较研究

从战略设计和领导机制、政策法规和保障措施等维度研究了美国、欧盟、俄罗斯、日本等发达国家和地区电子政务信息资源共享的安全保障政策。比较分析了我国电子政务信息资源共享的安全保障工作进展，提出了我国需要加强研究的几个突出问题。

3．电子政务信息资源共享的影响因素及安全风险分析

对电子政务信息资源共享的影响因素进行理论分析，确立实证分析上述问题的指标体系，对政府信息化管理层、各级政务信息中心、信息化服务机构、信

息咨询机构以及高校信息化领域的专家学者等进行问卷调研，分析了影响电子政务信息资源共享的主要因素，研究归纳了电子政务信息资源共享所面临的主要风险。

4．电子政务信息资源共享的安全保障机制建设案例研究

选取具有代表性的典型地区作为电子政务信息资源共享的研究案例，分析地方电子政务信息资源共享的安全保障机制建设的成功经验和存在的问题，总结其电子政务信息资源共享的安全保障机制建设方面的创新之处，研究和归纳出可在全国推广的普遍性措施。

5．电子政务信息资源共享的安全保障机制

结合当前我国电子政务信息资源共享的信息安全挑战和关键问题，以系统学的整体性、协同性、动态性安全观为指导，从宏观上设计构建电子政务信息资源共享的安全保障理论模型，并研究电子政务信息资源共享的安全战略保障机制、管理保障机制和技术保障机制。

6．推动我国电子政务信息资源共享安全保障机制建设的对策建议

结合我国国情，从加强战略统筹、明确顶层设计、健全管理体制、强化运行保障机制、实施自主创新战略等方面提出健全我国电子政务信息资源共享安全保障机制的对策建议。

第 2 章
电子政务信息资源共享与信息安全保障理论

2.1 基本概念

2.1.1 电子政务信息资源的概念和内涵

1. 电子政务

尽管众多学者和研究机构试图从不同的研究角度对“电子政务”的概念进行

界定，但是目前并没有关于“电子政务”统一的定义。从突出电子和网络技术应用的角度，“电子政务”可以被定义为“各级政府机构以电子和网络技术为基本手段，实现政务处理电子化，包括内部核心政务电子化、信息公布与发布电子化、信息传递与交换电子化、公共服务电子化等”[53]；从政府职能运行的角度考虑，联合国经济社会理事会将“电子政务”定义为“政府通过信息通信技术手段的密集性和战略性应用组织公共管理的方式，旨在提高效率、增强政府的透明度、改善财政约束、提高公共政策的质量和决策的科学性，建立良好的政府之间、政府与社会之间、社区以及政府与公民之间的关系，提高公共服务的质量，赢得广泛的社会参与度”；从组织结构转变的角度考虑，世界银行认为电子政务主要关注的是政府机构使用信息技术（如万维网、互联网和移动计算），赋予政府部门独特的能力，转变其与公民、企业、政府部门之间的关系。

综合以上定义，可以将“电子政务”理解为“政府为了适应经济全球化发展和政府行政体制改革的需求，利用先进的信息通信技术，通过自身业务流程改造提高工作效率和服务水平、通过信息公开提升工作透明程度和民主化进程、通过信息资源共享增强协调工作能力和消除信息孤岛的活动”。电子政务有以下几个方面的主要功能：

① 流程改造。主要是指政府内部借助信息化手段对业务流程进行梳理，提高工作效率。流程改造是在经济全球化条件下有效履行政府自身职能的必然需求。我国电子政务流程改造主要通过一些核心业务的信息化来实现，如“金字工程”的金关、金盾、金税等。

② 信息公开。要求政府和各组织机构向公众公开或开放自己所拥有的信息，使其他政府机构、企事业团体和公众个人可以基于任何正当的理由和采用尽可能简便的方法获得上述信息。我国政府信息公开的主要方式是门户网站。

③ 公共服务。体现了政务和政府的关系就是实现职能转变，推进行政体制改革，保证服务的公平、公开、公正、透明。我国电子政务公共服务主要体现在政府在线办事上。

[53] 朱桂棋．关于发展电子政务的若干思考[J]．中共浙江省委党校学报，2001（5）：67-70.

④ 协同共享。主要是将孤立的信息系统和分散的信息资源整合起来，发挥电子政务的整体优势，实现协同工作并消除数字障碍，提高电子政务的整体效能。目前我国电子政务协同共享主要通过跨部门信息资源共享和协同办公的项目来实践。

电子政务有三种业务模式：政府间的电子政务（G2G）、政府和企业间的电子政务（G2B）、政府和公众间的电子政务（G2C）。其中 G2G 是指上下级政府部门和不同政府部门之间的电子政务活动，其应用目标在于提升政府的工作效率和效力。本文研究的电子政务信息资源共享问题主要针对 G2G 模式的应用。

2．政府信息资源

从信息资源的内涵来看，有广义和狭义之分。美国著名信息管理学者霍顿（F.W.Horton）从政府文书管理的角度出发，认为信息资源是指“狭义的某种内容的来源，即包含在文件和公文中的信息内容，也可泛指支持工具，包括供给、设备、环境、人员、资金等”[54]。马费成、赖茂生从两个方面理解信息资源的内涵：狭义的“信息资源”是指在人类社会经济活动过程中经过加工处理有序化并大量积累后的有用信息的集合，如科技信息、政策法规信息、社会发展信息、市场信息、金融信息等，都是信息资源的重要构成要素；广义的“信息资源”是指人类社会信息活动中积累起来的信息、信息生产者、信息技术等信息活动要素的集合[55]。本文研究的电子政务信息资源指狭义的信息资源。

《中华人民共和国信息公开条例》等国家法规就将“政府信息”界定为“行政机关在履行职责过程中制作或者获取的，以一定形式记录、保存的信息”。政府是社会信息的最大拥有者，而且也是最大的信息生产者、消费者和发布者。政府信息资源为政务公开、业务协同、辅助决策、公共服务等提供了信息支持，是一切产生于政府内部或虽然产生于政府外部，但却对政府业务活动有影响的信息的统称。政府信息资源的开发利用是政府履行管理职能和进行科学决策的基础，是改善政务部门公共服务、建设服务型政府的重要条件，是政府各部门信息能力的集中体现，是电子政务应用系统有效运行和深入发展的前提。

[54] 卢泰宏，孟广均．信息资源管理专集[J]．国外图书情报工作，1992（3）.
[55] 马费成，赖茂生．信息资源管理[M]．北京：高等教育出版社，2006.2.

3．政府信息资源共享

根据《国家电子政务总体框架》（国信〔2006〕2 号）的界定，电子政务信息资源共享是指行政部门在履行职责过程中向其他行政部门提供，或从其他行政部门获取政府信息的行为。随着当前信息化、网络化的快速发展，高效的电子政务建设和管理要求政府信息资源在上下级间和部门间充分共享信息资源，以达到最佳的经济效益。政府通过整合和共享信息资源，满足经济社会发展的需要。

电子政务信息资源包括两个组成部分：一是政府自身产生的数字信息，如各种条例、规定、办法、章程、命令、指示、批复、议案、通告、通知、公函、会议纪要、合同、协议书等；二是政府从外部获取的与政府管理活动有关的数字信息，如社会调研信息、决策支持信息、提案议案、群众信访、统计数据、文献资料等[56]。针对不同的研究目的，对电子政务信息资源共享中的“信息”有不同的分类方法。例如，按照信息产生方式可分为政府与政府交往所形成的信息（G-G）、政府在商业中所形成的信息（G-B）、政府与公民交往所形成的信息（G-C）；按照信息获取方式可以分为政府机构在管理国家和社会事务的过程中所形成的信息，以及政府机构在管理国家和社会事务的过程中所收集的信息。由于政府信息的复杂性，无论从什么角度划分，各类信息之间并不存在严格的划分界限，彼此之间常常有交叉和重叠，甚至在时机成熟时互相转换。

① 信息资源共享与业务协同的关系。信息资源共享是业务协同的基础，业务协同是信息资源共享的动力。在电子政务中，由于政府职能部门的分工使得不同部门之间存在着信息差别，而业务协同能够有效提高工作效率，业务协同的基础是信息资源的共享，离开信息资源共享，业务协同就如“无米之炊”。随着我国电子政务建设的不断深化，业务协同所带来的社会、经济效益日益凸显，建设服务型政府要求业务协同的不断建设和深入发展，业务协同成为信息资源共享的动力之一。

② 信息资源共享与信息公开的关系。何振在国家社科基金项目“电子政务信息资源的共建与共享研究”中认为：电子政务信息资源共建共享的范围分为微观、

[56] 黄萃．基于门户网站的电子政务信息资源整合机制研究[D]．武汉大学，2005．

中观、宏观三个层次，即政府机关内部信息资源共建共享、政府系统之间信息资源共建共享和政府与社会之间信息资源共建共享，对于宏观层次的共建共享仅仅表示“在宏观层次上共建共享的信息资源是政府和社会互动的重要纽带”，并没有明确区分共建共享与政务公开之间的差别[57]。对于信息资源共享与信息公开之间的关系，结合政府信息公开的“以公开为原则，以不公开为特例”的理念，我们认为信息公开是信息资源共享的特殊表现形式。

2.1.2　信息安全保障的概念和内涵

随着信息化的高速发展，信息安全理论与技术不断更新和发展。信息安全从通信保密的基本要求逐步发展到今天对密码技术、信息对抗技术、系统生存技术和安全监控技术的综合需求。早在公元前 600 多年，Julius Caesar 就发明了一种简单的置换密码——恺撒密码，从而使得被截获的报文无法被非法使用者读出。1949 年，Shannon 发表了“保密通信的信息理论”，标志着密码学从艺术走向科学，从此进入了通信保密的研究时代。这一时期的研究强调的是对信息传输过程中保密性的要求[58]。1976 年，Diffie 和 Hellman 的《密码学研究的新方向》一文标志着公钥密码学时代的到来[59]。1977 年美国国家标准局公布了数据加密标准（DES），以及 1983 年美国国防部公布了可信计算机系统评价准则（TCSEC），对计算机信息系统的保密性提出了更高的要求。

利用公钥密码学的思想，密码学家提出了数字签名、消息认证、零知识证明以及安全多方计算等一系列新的密码学算法和协议，为基于信息的完整性、可控性和抗抵赖性的信息安全时代的到来奠定了技术理论基础。在 20 世纪 90 年代，美国政府宣布实施一项新的高科技规划——“国家信息基础设施（NII）”计划，其目的是以因特网为雏形，兴建信息高速公路，使所有的美国人方便地共享海量的信息资源。随着以“信息资源共享”为主要目的的因特网的使用，信息安全问

[57] 何振．电子政务信息资源的共建与共享研究[M]．北京：中国社会科学出版社，2009.
[58] C. E. Shannon. Communication theory of secrecy systems. Bell Sys. Tech. J. 1949, 28:657-715.
[59] W. Diffie, M. E. Hellman. New direction in Cryptography[J]. IEEE Trsns. Informat. Theory, 1976, Vol.IT-22(6): 644-654.

题逐步凸显。人们发现需要保护信息在存储、传输和使用过程中不被篡改和不被非法用户使用，保证信息的使用者和发送者不能否认自己的行为，以及对信息和信息系统实施安全监控等，信息安全对电子政务健康发展的推进作用由此显现。

随着社会信息化的不断深入和信息技术的快速发展，尤其是美国“9·11”事件后，人们对信息安全的需求更加强烈，信息安全的概念也随之得到了丰富。单一对信息的保护已经不能满足诸如网络恐怖活动和信息战等带来的安全问题，随之产生了信息安全保障的概念。信息安全保障不仅要求保证信息在存储、传输和使用过程中的保密性、完整性、可控性、可用性和抗抵赖性，同时要求把信息系统建设成一个具有预警、保护、检测、反应、恢复和反击等安全功能的纵深防御体系。图 2-1 展示了信息安全保障概念的演进。

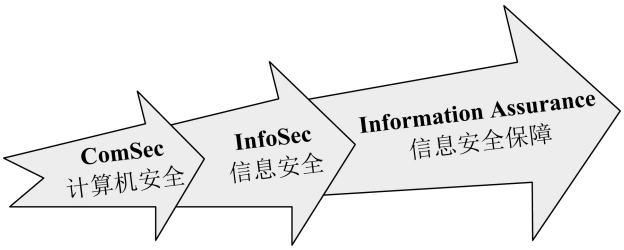


图 2-1　信息安全保障概念的演进

2.2　电子政务信息资源共享有关理论

2.2.1　基于系统学的视角

1．系统概念和复杂性科学

一般系统论的开创者贝塔朗菲（von Bertalanffy）将“系统”定义为“相互作用的多元素的复合体”。总体来说，如果一个对象结合至少有两个可以区分的对象，所有对象按照可以辨认的特有方式相互联系在一起，就称该集合为一个系统。按照系统结构的简单与否划分，可将系统分为简单系统与复杂系统两类。贝塔朗菲

于 20 世纪 40 年代末就提出研究复杂性的问题，预见到系统科学在一定程度上是研究复杂性的科学。20 世纪 50～60 年代，信息论、控制论、运筹学等技术科学研究得到了突破，而研究对象仍属于简单系统，尚未触及复杂性的实质。70 年代以后，关于简单系统的研究日趋成熟，系统科学才真正转向以复杂性为主的轨道。西蒙（Herbert A. Simon）把系统的等级层次结构与复杂性明确联系起来，指出等级层次结构是复杂性的重要来源。这些研究对后来的复杂性研究起到了积极的推动作用。

普利高津（I. Prigoginee）、哈肯（H.Haken）等人的贡献在于用演化的、生成的、自组织的观点解释复杂性。普利高津于 1969 年提出耗散结构理论（Dissipative Structure Theory）。普利高津在研究了大量系统的自组织过程以后，总结、归纳提出，系统形成有序结构需要一定条件：① 系统必须是开放的；② 远离平衡态；③ 非线性相互作用；④ 涨落现象。耗散结构是构造系统自组织特征的基础条件，自组织特征是事物作为一个活的系统的最基本特征。德国物理学家哈肯于 1969 年提出了协同理论（Synergetics），主要研究事物由无序变为有序的规律。协同理论认为，仅限于熵的概念去描述系统是不够的，因此提出了序参量的概念，并将系统的宏观结构和微观结构联系到一起。哈肯的贡献在于，他指出一个系统从无序转化为有序的关键不在于平衡和非平衡，也不在于离平衡态多远，而是由组成系统的各子系统，在一定的条件下，通过它们之间的非线性作用，互相协同和合作自发产生稳定的有序结构。耗散结构理论和协同理论从宏观、微观以及二者的联系上回答了系统本身走向有序结构的基本问题，二者都被称为自组织理论。

在 20 世纪 80 年代，我国著名科学家钱学森通过对系统科学及其应用的探索和研究，逐步认识到复杂性研究的重要理论和意义。他明确指出，凡是不能用还原论方法处理的或不宜用还原论方法处理的问题，而要用或宜用新的科学方法处理的问题，都是复杂性问题，复杂巨系统就是这类问题。

在方法论方面，钱学森于 1981 年对 Von Neumann 和 Morgenstern 所建立的博弈论，以及用 Monte Carlo 数值法在计算机上求得结果的方法进行了总结，提出能否把博弈论和系统科学结合起来用于结构复杂、成员众多的对阵集团。在后来的工作中对这一方法论赋予了更广泛的含义：处理复杂行为系统的方法，是科学理论、经验和专家判断力的结合。这种定量方法是半经验、半理论的，提出经验假

设是建立复杂行为系统数学模型的基础，这些经验性假设不能用严谨的科学方式证明，但需要经验性数据对其确定性进行检验。从经验性建设出发，通过定量方法途径获得结论。之后，通过在社会系统、人体系统和地理系统的研究实践，钱学森进一步提炼，提出了从定性到定量的综合集成法，其实质是将专家群体（各种有关的专家）、数据和各种信息与计算机技术有机结合起来，把各种学科的科学理论和人的经验知识结合起来。这种方法的成功应用，就在于发挥了系统的整体优势和综合优势。

2．电子政务系统的构成要素分析

基于系统学方法，本报告认为电子政务系统是由政务网络、政务信息和政务用户三个最为基本的要素构成的。下面分别加以分析。

（1）政务网络

计算机网络研究已经引起学者的广泛重视：在信息科学家看来，计算机网络是用于信息采集、信息存储、信息传输、信息处理的工具和载体。社会科学家研究计算机网络中人的行为模式及网络文化。地理学家探讨信息技术应用对地理空间的影响，提出了数字地球的概念。从社会和系统科学的角度分析，可以将计算机网络看作一个典型的、具体的开放复杂巨系统实例。计算机网络作为一个开放的复杂巨系统，特别是其与社会政治、经济与意识形态之间的密切联系，突显出就有关问题进行系统研究的必要性。对计算机网络的内在特征加以分析，有助于我们更具体地研究、分析其对社会发展和社会安全的影响和作用。将计算机网络技术应用于政府工作，就构成了电子政务网络。政务网络有以下系统学特征：

① 异构性。政务网络包括政务外网、政务内网、政府专网，各种网络在数据传输速率、数据帧格式和长度限制、网络协议、网络流量控制、服务质量、安全保障等方面存在着差异。

② 交互性。政务网络是一个开放的系统，在系统运行的整个生命周期中，网络与用户之间、网络与网络之间不断发生交互作用，使得政务网络呈现出交互性的特点。

③ 层次性。政务网络包含多个子系统，各个子系统的功能、结构不同，子系

统之间的交互形式、内容各异，系统间的协同作用表现不一，使得政务网络显示出层次结构复杂性的特点。

（2）政务信息

电子政务信息则是指政府在履行职能过程中产生或使用的信息，为政务公开、业务协同、辅助决策、公共服务提供信息支持。在信息时代，政务信息成为国家的重要战略资源，政府信息能力也成为国家能力的重要体现和保障。政务信息有以下特性：

① 敏感性。政务信息事关国家安全和公民的隐私，在使用和处理过程中表现为极强的敏感性特点。

② 保密性。很多政务信息涉及国家秘密，如果被非授权使用，则会损害国家利益，危及国家安全。

③ 流动性。政务网络是一个大的开放系统，由多个网络组成，包含多个子系统，各系统中产生和存储的信息复杂多样。为实现电子政务的公众服务、社会管理和协同办公功能，就需要政务信息在网络内部、跨网域之间实现传输和交换。

④ 经济、社会价值突出。政务信息多为政策法规、行政指令、统计数据等内容，这些信息是政府决策、日常管理、宏观调控、社会管理的重要依据，如果被利用得当，则会表现出突出的经济和社会效益。

（3）政务用户

信息的强大力量和特征，加上人的智慧和网络全球化的载体，形成巨大的力量，在未来社会事业发展中将发挥重大的作用。信息网络作为一个开放的复杂巨系统，表现出很高的智能性，它是一个人-机结合、人网合一的“人造”系统，在这个系统中人扮演着主导角色。“人”作为这个复杂巨系统的创建者、使用者和管理者，同时也可能是系统的破坏者和攻击者，“人”是电子政务系统中最为活跃的因素，也是形成网络智能的原动力。政务用户具备以下特性：

① 多样性。政务用户涉及政务工作人员、公民、企业用户，具有多样性的特点。

② 复杂性。政务用户涉及多种类型，不同类型之间的用户权限不用，同一类型的用户之间也可能存在权限方面的差异，具有复杂性的特点。

3．电子政务信息资源演化的系统学分析

（1）协同理论

电子政务作为一个开放的巨系统，由大量的子系统组成，电子政务系统中的信息资源共享和业务子系统之间的协同符合协同理论的基本规律，二者的协同作用使得电子政务系统发生非平衡相变，在序参量、涨落等的共同作用下，最终达到自组织状态。

电子政务建设的初始时期，无序化使得公共服务效果较差，信息孤岛丛生，推动电子政务建设有序化的关键是找出序参量。电子政务系统依赖于业务流的输入和输出，业务需求是推动业务流中信息资源不断被应用，从而实现输出的一个流程，是信息资源进行不停交换的动力[60]。在交换过程中，需要电子政务信息资源共享子系统与业务子系统在技术能力、信息安全保障、标准、管理机制等一系列因素上协同合作，从而构成电子政务系统从无序走向有序的序参量。

涨落现象是系统形成有序结构的必要条件之一。电子政务系统作为一个庞大的复杂性系统，在发展过程中常常会表现出涨落现象。例如，用户对系统的新需求、新信息技术的出现和新法规的颁布等。当这些涨落现象结合系统内部人员的认知及技术行为的涨落时，可能会产生一种远离平衡态的变化[61]。在我国电子政务信息资源共享建设的过程中，从基础设施建设阶段到信息资源整合阶段，再到目前的信息资源共享平台建设阶段，期间无不伴随着新需求、新技术的出现和新法规的颁布带来的涨落现象。

（2）耗散结构理论

耗散结构是一个动态、稳定的有序结构，系统可以从一种耗散结构向新的高

[60] 张新宇，罗贤春．基于协同学的电子政务信息资源共享与业务协同的协同模型及实现[J]．图书馆情报工作，2011（1）：126-129．

[61] 雷银枝，李仁爱．协同学视角下的电子政务协同过程研究[J]．图书馆情报工作，2009（5）：122-126．

级的耗散结构跃迁和发展。系统要维持有序状态，必须满足耗散结构的形成条件[62]：系统是开放的；系统内部必须存在非线性的相互作用；系统必须是涨落有序的；系统应该是远离平衡态的。耗散结构理论为研究和分析电子政务信息资源共享提供了理论基础。从耗散结构的理论分析来看，电子政务系统是一个开放的系统，系统内部的子系统之间存在着非线性的相关作用，通过电子政务信息资源建设的不断推进达到涨落有序。由于电子政务信息资源共享的业务需求和相关信息技术的不断更新，系统处在远离平衡的状态。

2.2.2　基于信息经济学的视角

电子政务信息资源共享能够提高政府工作的执行力、政策实施力，不断改善政府的管理和服务，提高政府办事效率，方便公众。信息经济学中的信息不完全与非对称性和信息资源共享与可再生原理是推动电子政务信息资源共享的动力。

1．信息不完全与非对称性

信息不完全与非对称性是信息经济学的基本前提与观点[63]。在现实经济环境中，市场参与者一般不拥有某种经济环境的全部信息，同时，市场参与者拥有的信息也是有差异的，这种信息存在的规律称为信息不完全与非对称原理。不对称信息的存在是对社会专业化分工的肯定，是社会劳动分工和专业化在经济领域的具体表现。信息不完全与非对称原理意味着信息的不完全与非对称是一种不能消除的现象，同时为信息赋予了经济属性，这也在一定程度上为电子政务信息资源共享问题的研究提供了理论指导。

在电子政务实践中，由于政府职能部门的分工使得不同部门之间产生了信息差别，也产生了信息优势与劣势，即存在着信息不完全与非对称。电子政务中信息的不完全与非对称性，催发了电子政务信息资源共享的需求。

[62] 王山．政府耗散结构的理论分析[J]．成都行政学院学报，2009（6）：80-82.
[63] 靖继鹏等．信息经济学[M]．北京：科学出版社，2007.

案例 1　劳动部门负责的“养老金”发放服务

由于受益人的居住地具有分散性，受益人的生活方式具有变动性，对其死亡、迁移、失踪、获刑等的信息，劳动管理部门由于职能所限往往不能及时掌握，导致养老金多额、冒领现象经常发生，并且该项服务的效率低下，劳动管理部门的纠错过程费时耗力。如果劳动管理部门与民政、公安、司法、劳动等相关职能部门共享人口的死亡、迁移、失踪、获刑等基本信息，就能克服服务受益人信息分散带来的服务和管理困境。

据东南网 - 海峡导报 2010 年 9 月 5 日讯，福建省人力资源和社会保障、民政、公安、财政四部门日前联合建立死亡人员信息资源共享机制，开展城镇企业职工基本养老保险、机关事业单位养老保险、农村社会养老保险养老金领取资格认证，从根本上杜绝活人冒领死亡人员养老金的问题。据了解，此次福建省建立死亡人员信息资源共享机制，主要由市、县（区）民政部门负责采集各殡仪馆死亡人员基本信息，公安部门采集死亡人员户口注销信息，人力资源和社会保障部门指定经办机构每月收集汇总民政、公安部门当月死亡人员信息和基层劳动保障平台上报的新增死亡人员信息，依托共享资源，核实养老金领取资格，防止死人继续领养老金，维护基金安全[64]。

通过案例 1 可以得出，信息资源共享能够克服由于政府职能部门之间分工不同造成的信息不完全与非对称性对电子政务工作带来的困难。通过人力资源和社会保障、民政、公安、财政四部门之间的信息资源共享，解决了活人冒领死亡人员养老金的问题。

2．信息可再生原理

信息经济学中的信息可再生原理是指，信息可以由多人在同一时期或不同时期占有和使用，而不改变其价值及性质，并且在信息传播的过程中，可以在原有的信息基础上产生新的信息。它包含两方面的含义：

① 信息具有共享性。信息的共享性是指信源发出的信息经传递和转换作用可

[64] 资料来源：东南网–海峡导报，2010-09-05。

以为广泛的接收者所享有，而信息量不变的性质。具体包括：

a．同一信息可以为许多人所共享。

b．同一信息可以为不同时期的人所共享。

② 信息具有再生性。信息的再生性是指在原有信息的基础上可以产生新的信息，实现原有信息的增值。信息的再生性是信息不守恒的最突出表现，信息通过不守恒性，与物质和能量严格区分开来。

由此可见，信息不仅是可以共享的，并且信息可以再生出新的信息；信息资源共享的范围越大，信息使用成本越低，信息的效率就越高，信息的作用就越大；信息可再生能力越强，创造出的新信息就越多，信息在经济社会发展中的作用就越大。

该原理同样适用于电子政务信息资源共享中。电子政务中共享的信息资源范围越大，信息利用成本越低，信息效率就越高，信息作用就越大。

案例 2　广州市地税与工商部门查处“漏登”、“漏征”户

在开展信息资源共享之前，对于只领取工商营业执照而未领取税务登记证的“漏登”户，税务部门缺乏一种有效、快捷的掌握办法。企业基础信息资源共享后，创造性地提出了“信息预警”模式：通过将广州市工商局提供的企业登记信息和市地税、国税局提供的税务登记信息实时比对，可发现领取工商营业执照后超过 30 天仍未办理税务登记的企业，列入“应办未办税务登记”预警企业名单，由税务部门调查处理，有效减少“漏登”、“漏征”户的产生，从源头上加强税源监控。2008 年，累计发现应办未办税务登记企业 1.7 万多家，实际催办补登效率超过 80%，目前全市企业的税务登记率超过 94%。2008 年上半年，广州市地税局组织税费收入突破 500 亿元，同比增长 23.4%。

与此同时，税务部门大大缩短了办事时间。市工商局登记的新注册成立的企业信息通过市电子政务数据中心交换给市质监局、市地税局和市国税局，减少了企业信息的重复录入，把以前 10～20 分钟的业务办理时间缩短到 2 分钟，提高了

税务登记工作效率，同时也方便了企业登记人[65]。

由案例 2 可以看出，通过企业基础信息的共享，税务部门大大缩减了办事时间，提高了税务登记工作效率，同时也方便了企业登记人。这一案例说明了电子政务中的信息资源共享能够降低信息利用成本，提高信息的效率和作用。

3．信息资源共享效率

信息效率是反映信息发挥作用的程度，是经济进步和社会发展的重要因素。按信息获取的环节来考察，信息效率包括信息采集的效率、信息传输的效率、信息处理的效率和信息资源共享的效率等。乌家培认为，在信息资源稀缺的情况下，研究信息效率问题，易于为大家所接受。相反，在“信息爆炸”的环境下，人们常常忽视信息效率问题。在政府信息资源共享问题被普遍提到工作日程的条件下，应该同样重视信息资源共享的效率问题。

（1）成本收益原理

从成本收益的原理出发，当共享信息收益大于成本时，信息资源共享才有意义；当边际收益大于边际成本，共享该信息可以获得利润时，信息资源共享才有意义；在边际成本和边际收益相交点，共享该信息可以获得最大利润。因此，从信息经济学角度考虑，信息资源共享不是全部共享，而是有条件、有选择的共享。目前，在电子政务信息资源共享工作中，尚缺乏对于信息资源共享效益的评估。

（2）资源配置

信息资源作为一种重要的资源，具有经济资源的最基本特征，即稀缺性，表现为生产信息资源的投入（成本）和转让信息资源的产出。从信息经济学角度来分析，信息资源共享应该是提供者和使用者之间包括成本的分担和收益的分配的利益均衡。电子政务信息资源共享从本质上可以看作一种资源配置方式，即在电子政务中的特定条件和环境下，对一定范围内的电子政务信息资源进行重新组合

[65] 资料来源：中国政务信息化网[2011-10-20]．http://www.chinaeg.gov.cn/html/detial/magazine/201010/201010111433078796.html。

和优化配置，以提高信息资源的利用效率。

从资源配置的角度出发，当前电子政务信息资源共享中还存在一些问题，影响了共享的推进。主要包括：① 区分共享与非共享电子政务信息资源；② 区分有偿共享与无偿共享电子政务信息资源；③ 电子政务信息资源共建共享的效益、效率问题；④ 电子政务信息资源共建、共享与整合之间的关系等。

2.2.3　基于信息管理学的视角

信息管理学中的“共享原则”是指，在信息管理活动中为获得信息潜在价值，力求最大限度地利用信息的管理思想。共享性是信息的基本特征，共享能够发挥信息潜在的价值。

电子政务信息资源共享一方面能够将政府管理和服务中的综合性信息反馈给政府决策机构，以优化和调整相关行政法规、政策和制度，进而形成政府决策机构对政府职能部门间信息资源共享和业务协同的压力，以提高行政执行力、政策实施力、政策实施的准确性和有效性，进而不断改善政府的管理和服务；另一方面，电子政务信息资源共享能够使相关职能部门协同、高效地完成政务业务工作，提高政府办事效率，方便公众。特别是在应对突发事件时，电子政务信息资源共享的作用显得尤为突出。在突发事件面前，信息资源共享能够避免产生信息孤岛，为快速、有效地处理突发事件提供必要的支持。

1．动力机制

（1）现代信息技术驱动

自 20 世纪以来，以现代信息技术为核心的新技术革命给人类社会生活的方方面面带来了深刻影响。计算机技术、通信网络技术、微电子技术等现代技术的快速发展，从根本上改变了信息产生、传递和利用的方式，增强了信息处理、存储、传播、服务等过程的能力和效率。信息技术，特别是网络、数据库等，以及各种软件的发展和应用，使得网络化的信息系统成为可能。信息系统的最大作用在于改善政府各职能部门工作的协同性，大大提升政府组织对外部环境变化的适应能

力。如今，政府的各项业务可以通过信息系统来实现，通过信息网络与全国各地的连接，实现各个政府机构间的协同工作和信息资源的共享。

近年来，随着以网络和通信技术为代表的信息化技术的不断发展，各种新兴技术日新月异，各种应用领域层出不穷。从 IPv4 到以 IPv6 为核心的下一代互联网，从互联网到泛在网，从传感网到物联网再到“智慧地球”，从网格计算到云计算，从社区计算到社会网络，从第三代移动通信技术（3G）到第四代移动通信技术（4G），信息化技术渗透到电子政务工作的各个方面，对电子政务信息资源共享的发展和建设带来了深刻的影响。在电子政务信息资源共享的发展和建设过程中，现代信息技术作为核心驱动力正日益发挥着巨大的作用。

（2）政府行政体制改革的需求

电子政务信息资源共享是建设法治政府的需求。法治政府建设是政府从决策到执行及监督的整个过程都纳入法制化轨道，权利与责任紧密相连，集“阳光政府、有限政府、诚信政府、责任政府”于一身，并用法律加以固定。推进法制政府建设，政务信息资源的公开透明是基础，政务信息资源的共享能够促进法治政务的建设。

电子政务信息资源共享是建设服务政府的需求。信息资源共享是政务业务部门协同的必要条件，业务协同则为“以服务为导向”的政府工作方式的转变提供了基础。政府的基本职能包括经济调节、市场监管、社会管理和公共服务，政府施政的最终目的是服务社会。电子政务信息资源共享能够优化政府服务，有助于推进服务型政府建设。

电子政务信息资源共享是建设效能政府的需求。效能政府建设致力于高效率的工作和能力，清正廉明，较好地为公民服务。建设效能政府，其关键问题是政务工作效率的提高。电子政务信息资源共享能够加强政务部门之间的业务协作并提高工作效率，极大地满足了效能政府建设的需求。

2．推行阻力

针对电子政务信息资源共享的现状和困难，我们从行政阻力和技术风险两个方面对电子政务信息资源共享推行阻力作一些理论探讨。

（1）行政阻力

电子政务信息资源共享的行政阻力的根源来自不同级别的政府及其职能部门的行政影响，即政府权力意志的指向与实现[66]。电子政务信息资源共享的行政阻力主要表现在以下几个方面：一是由于政府部门分工不同带来的信息不对称，使得一些政府部门有本部门信息资源获得的独特渠道，出于维护本部门的权威，部门会以各种理由阻碍信息资源共享[67]。二是信息资源共享建设需要大量投入，一方面，当一些政府部门加大信息资源共享投入而得不到补偿时，会对信息资源共享建设持消极态度；另一方面，一些政府部门为保护已有的投入，不愿修改现有的信息系统来适应信息资源共享的要求。三是由于信息资源共享增加管理的复杂性和安全风险，一些拥有独立信息系统的政府部门不愿将信息资源共享互联。

面对电子政务信息资源共享现有的行政阻力，我国从电子政务建设的顶层设计出发，指导电子政务信息资源共享建设。中共中央办公厅 17 号文件提出要提高信息资源共享的程度；“十二五”规划提出要“以信息资源共享、互联互通为重点，大力推进国家电子政务网络建设”。

（2）技术风险

在电子政务信息资源共享中，不同领域的关键信息以数字化方式进行存储和处理，大量事关国家安全和公民隐私的敏感信息在共享中传递，信息安全风险的存在对电子政务信息资源共享建设产生着一定的影响。

政务信息资源事关国家政治安全、经济安全、国防安全和社会稳定，如果被泄露或被不正当利用，则会对国家安全、公民隐私、单位财产构成严重威胁，后果不堪设想。《联合国电子政务调查报告 2008》指出，在互联政务的框架下，系统地收集、重新使用与分享数据和信息。互联政务的关键是建立协同工作的概念，使政府组织能够按通用标准分享和整合数据。并认为，“安全是影响人们使用电子政务服务的主要因素”。信息资源共享和业务协同给电子政务信息安全保障带来很大的挑战。当前，我国电子政务信息资源共享和业务协同能力不强问题突出，各

[66] 张新宇，罗贤春．电子政务信息资源共享研究综述[J]．国家图书馆学刊，2009（2）：59-62.
[67] 胡小明．电子政务信息资源共享的经济学研究[J]．中国信息界，2004（17）：14-15.

部门丰富的信息资源还没有形成共享机制。其中一个重要的问题就是信息安全问题或对信息安全的信心难以得到保障。电子政务是一个多域环境。电子政务架构的特点是不同类型政府机构间存在不同的安全策略，从而构成一个高度异构的多域环境。由于每个机构电子政务系统的安全目标不同、处理信息的敏感级别不同、面向的服务对象不同，使得电子政务系统之间的跨域访问和信息交换与共享问题十分复杂。这不仅要依赖身份认证、访问控制等技术手段，更重要的是需要从战略层面规划设计出系列性的标准体系和政策法规。

此外，由于政府信息资源中涉及公民隐私相关的信息，电子政务信息资源共享也面临着隐私安全的挑战。一是在政府与社会之间的信息资源共享中，政府通过发布信息来为公众服务。在信息发布中，如果不考虑信息披露的必要性和充分性界限，过度披露有关当事人的隐私信息，就会触犯当事人的合法利益，甚至使当事人在当地无法生活或无法生存。但是如果有些该披露的信息不充分发布，就会让社会产生各种猜度，长此以往，政府的公信力就会大打折扣。二是在政府部门之间的信息资源共享中，当需要政府部门之间共享信息协作完成政府业务时，就面临着数据挖掘中的隐私保护问题、信息资源共享过程中的隐私安全问题等。三是在政府机关内部信息资源共享中，对于政府机关内部涉及隐私信息的共享，可能会出现对隐私信息访问权限的授权管理不当所带来的隐私安全威胁。

2.3 电子政务信息安全保障有关理论

2.3.1 信息安全模型

信息安全的目标就是要保证信息系统中信息的保密性（C，Confidentiality）、完整性（I，Integrity）和可用性（A，Availability），其中：

① 保密性主要指未经授权的用户不能读取保密信息。

② 完整性主要指数据和计算机程序（或软件）的完整性。数据的完整性是指在未经授权的情况下不能被修改或删除；程序或软件的完整性是指软件程序不能

被恶意敌手或病毒修改。

③ 可用性主要指计算机可以以我们所期望的方式和时间正常运行。实际上，可用性还需要软件可靠性和容错计算等的支持，尽管它们都不属于安全的研究范畴。在安全领域，可用性就是要保证攻击者无法阻止合法用户对其计算机系统进行访问。

信息安全领域的重要理论模型主要包括以下几种。

1．Bell-LaPadula 模型

Bell-LaPadula（简称 BLP 模型）是一个以模型的提出者 D.Bell 和 L.LaPadula 命名的多级安全模型，该模型是第一个将实际系统的属性转化为规则的数学模型[68,69]，并且在很大程度上影响了计算机安全理论和技术的发展。美国国防部的可信计算机评估准则（Trusted Computer System Evaluation Criteria，TCSEC）就是基于这一模型开发的。BLP 模型要解决的本质问题是对具有密级划分的信息的访问进行控制，该模型结合了强制访问控制和自主访问控制。

BLP 模型是一个对计算机安全产生深远影响的安全模型，但它同时存在以下缺点：

① BLP 模型只关注信息的保密性，而忽视了信息的其他安全属性，并且保密性是建立在军方系统的安全分类模型之上的。因此，BLP 模型本身不是一个完整的信息安全模型。

② 该模型假设信息的保密级别一旦确定，这种分类将永不改变，现实世界并不是这样的。因此，该安全模型缺乏必要的灵活性。

③ BLP 模型的提出受限于当时的应用环境，因此，其描述对象主要指单机和多用户分时计算机系统。

---

[68] D.Bell, L.Padula. Security Computing Systems: Mathematical Foundation and Model. MITRE Report, Bedbord, MA, 1975.

[69] D.Bell, L.Padula. Security Computing Systems: Unified Exposition and Multics Interpretation. Technical Report MITRE-2997 Rev.1, Bedbord, MA, 1975.

2．Biba 完整性模型

Biba 模型是一个关注数据完整性的模型，也是一个基于信息流的模型，它阻止信息从低完整性等级的客体流向高完整性等级的客体。Biba 提出了三种完整性策略：low-water-mark 策略、环策略和严格完整性策略。其中，严格完整性策略是 BLP 模型在数学上的对偶。因为保密性规定谁可以看到信息，而完整性研究谁能够创建和更改信息。只有用户的安全级别高于数据的安全级别时才可对数据进行写操作；相反地，只有用户的安全级别低于数据的安全级别时才可读取该数据。信息在系统中只能自上而下地流动，以此来保障信息的完整性。

3．Clark-Wilson 完整性模型

Clark-Wilson 模型是 1987 年由 David Clark 和 David Wilson 提出的一种完整性模型，它关心的是数据的有效性、可验证性和访问控制等问题[70]。

Clark-Wilson 模型给出了多数商业公司处理数据的方法，它以“约束”数据项为中心，要求主体只能用规定的方式对数据进行操作。模型把计算机系统中的数据分为两类：一类是需要实施完整性控制的数据，称为约束数据（Constrained Data Items，CDI）；另一类是不属于完整性控制的数据，称为非约束项（Unconstrained Data Items，UDI）。Clark-Wilson 模型通过结构合理的（Well-formed）事物处理和职责分离两个基本原则来保证数据和系统的完整性。事物处理是指用户不能任意操纵数据，只能以约束的形式控制数据。职责分离则要求检验者和实现者不是同一个人。数据的完整性是指一个系统中数据的正确性、真实性和精确性。系统的完整性是指对信息资源的正确操作。此模型把证明（Certification）的概念和实施（Enforcement）的概念分开，并分别给它们赋予了各自的规则，分别称为证明规则和实施规则。前者是完整性策略的安全管理者使用，后者是由系统来实施。

4．中国长城模型

中国长城（Chinese Wall，CW）模型是由 D.Brewer 和 M.Nash 提出的一类多

[70] D.D. Clark, D.R. Wilson. Non Discretionary Controls Commercial Applications[C]. Proc. of the IEEE Symposium on Security and Privacy, 1997:184-194.

边安全模型[71]，该模型是一类同时考虑保密性和完整性的混合安全模型，它在商业领域的作用与 BLP 模型在军事领域具有相当的重要性。CW 模型设计的理念很直观。CW 模型有三个概念层次：

① 最底层考虑的是与某家公司相关的信息条目，与 BLP 模型相一致，称存储这些信息条目的文件为客体。

② 在中间层，把涉及某家公司的所有客体组合到一起，称为公司数据集。

③ 在最高层，把所有存在利益冲突的公司归类，称为利益冲突类。

CW 策略的基础是用户能访问的信息必须与其已经拥有的信息不存在冲突关系。就计算机系统而言，用户拥有的信息包括用户计算机中存储的信息和用户已经访问过的信息。CW 策略假设一个没有访问过任何信息的用户不存在利益冲突问题，提出了 CW 简单安全性质和 CW-*-性质。

2.3.2　信息安全保障体系模型

1．McCumber Cub 及其扩展模型

McCumber Cub 模型的方法理念是将信息状态分为信息的存储状态、信息的传输状态和信息的处理状态，并将一个立方体划分为不同的小立方体，用每一个小立方体来定义针对某一类信息状态的安全保护策略[72]（见图 2-2）。该模型全面描述信息安全的三维模型，包括安全服务维（可用性、完整性和保密性）、安全措施维（技术措施、策略和实践措施、人员措施）和信息状态维（存储状态、传输状态和处理状态）。

[71] F.C.B. David, .N. Michael. The Chinese wall Security Policy[J]. IEEE Symposium on Research in Security and Privacy, 1989:206-214.

[72] J. McCumber. Information Systems Security: A Comprehensive Model[C]. Prco. Of the 14th National Computer Security Conference. NIST. Baltimore, MD. 1991.10.

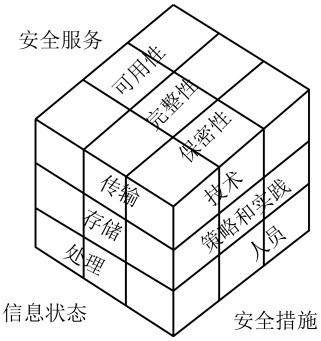


图 2-2　McCumber Cub 模型

W.V.Maconachy 等引入时间的概念[73]，将 McCumber Cub 模型扩展成为一个动态的信息安全保障模型。该模型包括安全服务维（可用性、完整性、保密性、可认证性和抗抵赖性等）、安全措施维（技术、策略和实践、人）、信息状态维（传输、存储和处理）和时间维四个维度。该扩展模型不仅刻画了信息安全的各个要素，而且更强调各要素之间的相互作用机理。

2．基于时间的 PDR 模型

W.Schwartau 在 1998 年给出了一个基于时间的 PDR（Protection-Detection-Response）信息安全模型[74]，也称作 TSB（Time-Based Security Model）模型，旨在为信息系统的信息安全效果和效益提供一个量化的、逻辑性强的、可证明的测度模型，以实现信息安全的科学管理。基于时间的 PDR 模型的基本理念是，承认信息系统的任何防护措施都是可以攻破的，都是基于时间的，一切防护措施都不是永久安全的。

3．P2DR 模型

P2DR 安全理论模型作为信息系统安全体系构建的基础，也称为可适应网络安全理论模型。P2DR 模型是在整体的安全策略的控制和指导下，在综合运用防

[73] W.V. Maconachy, C.D.Schou. A model for information assurance: an integrated approach[C]. Proceedings of the 2001 IEEE Workshop on Information Assurance Security. NY, 2001:180-185.

[74] W.Schwartau. Time-based security explained: Provable security models and formulas for the practitioner and vendor[J]. Computers & Security, 1998, 17(8): 693-714.

护工具（如防火墙、身份认证和加密等）的同时，利用检测工具（如漏洞扫描、入侵检测等）了解和评估信息系统的安全状态，通过适当的反应将系统调整到“最安全”、“风险最低”的状态。P2DR 模型包括 4 个主要部分：Policy（策略）、Protection（防护）、Detection（检测）和 Response（响应）。防护、检测和响应组成了一个完整的、动态的安全循环，在信息安全策略的指导下保证系统的安全，如图 2-3 所示。

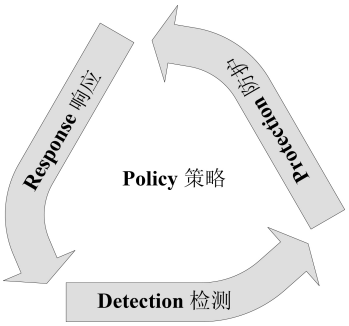


图 2-3　P2DR 模型

4．WPDRRC 模型

基于信息安全的多维性、动态性和对抗性，国内信息安全专家对 PDRR（Protect-Detect-React-Restore）信息安全保障模型进行了改进，得到了更为直观的信息安全保障结构，即 WPDRRC（Warning-Protect-Detect-React-Restore- Counterattack）模型（如图 2-4），它代表了信息安全保障预警、保护、检测、反应、恢复和反击六个环节。该模型融入预警和反击体现了信息安全保障是一个动态、博弈的过程，强调对信息系统安全的控制、定位、追踪、监管和对抗能力。

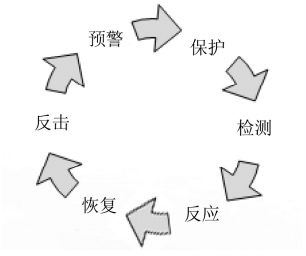


图 2-4　WPDRRC 模型

5．IATF 定义的深度防御模型

《信息保障技术框架》（IATF）是由美国国家安全局发布的[75]，最新的 3.1 版本于 2002 年 9 月推出。IATF 从整体、过程的角度看待信息安全问题，其代表理论为“深度防护战略（Defense-in-Depth）”。IATF 强调人、技术、运行这三个核心要素，关注信息安全的四个保障领域：保护网络和基础设施、保护边界、保护计算环境、保护支撑基础设施（见图 2-5）。

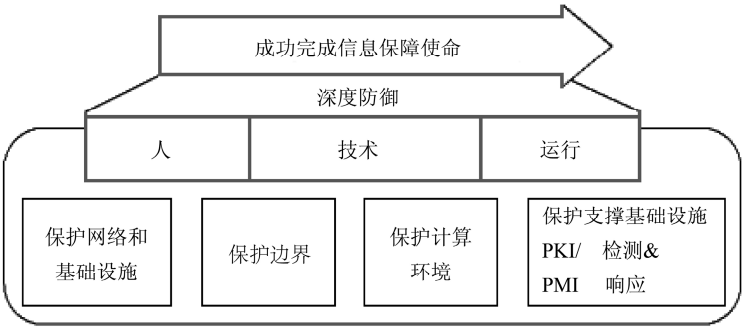


图 2-5　IATF 定义的深度防御模型

IATF 定义的信息保障体系包含人、技术和运行三个要素，根据信息保护策略的违反造成的影响把信息的价值分为五个等级，并定义了包括被动攻击、主动攻击、物理临近攻击、内部人员攻击、软硬件装配分发攻击在内的五类攻击。

2.4　电子政务信息资源共享与信息安全保障的关系分析

2.4.1　电子政务信息资源共享中的矛盾关系分析

基于系统学的分析，本研究发现在电子政务信息资源共享中存在如下的矛盾关系。

[75] Information Assurance Technical Framework 3.1[R]. National Security Agency Information Assurance Solutions Technical Directors, 2002.9.

1．信息的生产者与使用者权益之间的关系

电子政务信息资源是政府在履行职能过程中产生或使用的信息。在政务信息资源的生产和使用过程中，信息的生产者付出了一定量的劳动，因此需要平衡信息的生产者与使用者权益之间的关系。

2．政府机密与公众利益之间的关系

一方面，电子政务信息资源涉及政府机密，事关国家安全，保守和保护政府机密是公务员和公民的天职，涉及国家安全的政务机密是不能公开的；另一方面，公众有权了解政府是如何运作的，以及在一定程度上参与政府决策并对政府进行监督。因此，需要平衡政府机密与公众利益之间的关系。

3．信息资源共享与个人隐私保护之间的关系

信息资源共享是信息自由流动的表现形式。在电子政务信息资源共享中，信息可能涉及公民隐私，因此，有必要平衡信息资源共享与个人隐私保护之间的关系。

2.4.2　电子政务信息资源共享中的安全风险分析

基于系统学分析，本研究认为电子政务信息资源共享的安全风险包括：

1．政务信息的跨网域共享及其安全风险

电子政务信息资源共享涉及信息在网络中的流动，政务网包括政务内网、政务外网、互联网，各个网络中流动的信息级别不同，不同敏感级别的政务信息的跨网交互使用将面临着一定的安全风险。

2．政务用户的跨网域协同及其安全风险

在政务信息资源共享中，政务用户常常跨网域访问，不同网域之间的安全策略往往不尽相同，政务用户的跨网域访问面临着诸如身份假冒、身份盗窃等安全威胁。

3．政务用户对信息的处理及其安全风险

政务用户对政务信息资源的处理涉及信息的整个生命周期，包括信息的存储、传输、交换、处理等各个阶段，信息泄密、移动介质误用及信息资源的授权管理等安全风险始终存在。

2.4.3 电子政务信息资源共享与安全的博弈和平衡分析

基于信息经济学分析，本研究认为电子政务信息资源共享与安全的博弈和平衡关系包括以下两个方面。

1．共享与安全的博弈分析

收益与风险是一对矛盾，电子政务信息资源共享能够节省信息重复采集带来的巨大开支，提高政府部门之间的协作效率，加快服务型政务建设的步伐，为电子政务建设带来良好的经济和社会收益，但是与此同时，共享带来的安全风险也不容忽视。

随着共享内容的增多、范围的增大以及共享的紧密程度的增加，安全风险直线上升，因此并不是所有的信息资源共享在经济上都是合算的，很多信息资源共享系统是亏损的，其所取得的收益不足以冲抵该共享系统的安全风险成本。过度的共享会带来较大的安全风险，并使得系统长期的经济效益降低。在电子政务信息资源共享中，不同领域的关键信息以数字化方式进行存储和处理，大量的事关国家安全和公民隐私的敏感信息在共享中传递。信息资源共享致使系统的安全成本上升，信息资源共享的密集型越强，系统越复杂，其安全风险也越大。

Ulrich Beck 在《风险社会》一书中提到，每个利益团体都试图通过风险的界定来保护自己，并通过这种方式去规避可能影响到它们利益的风险。电子政务信息资源共享是双向或多向的，这就决定了共享过程中会触及利益，并带来相应的安全风险。共享与安全实质上是一种博弈关系，共享的目的是电子政务业务部门获得最大的收益，在获得收益的同时伴随着安全风险。以部门之间的信息资源共享为例描述：部门 A 和部门 B 需要共享一定的信息资源进行业务协作，共享信息

资源的收益由 a 表示，代表着数据采集等的建设成本的降低、政务效率的提高，以及电子政务服务质量的提高；共享带来的风险由 b 表示，代表着因共享带来的信息安全技术相关的风险和管理风险。博弈的行动是共享和不共享，博弈的主体是部门 A 和部门 B，如图 2-6 所示。

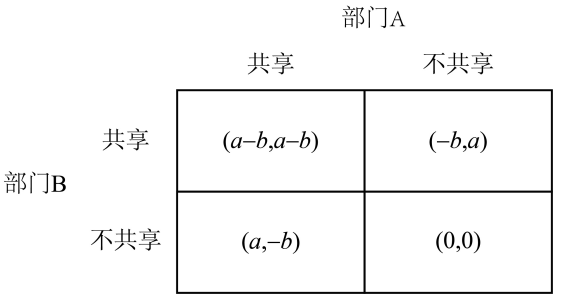


图 2-6　部门间信息资源共享的博弈

如果部门 A 与部门 B 共享信息，则双方都能得到因共享带来的成本降低、政务效率提高和服务质量提高这一收益，与此同时，双方共同承担着信息安全相关的风险 b；如果只有一个部门共享信息而另一个部门不共享，则提供共享的部门将面临着信息安全相关的风险 b，不提供共享的部门独获因共享产生的收益 a。显然，这对提供共享的一方而言是无收益而有风险，除非该信息资源是电子政务活动中的行政手段强制规定的；否则，从经济学角度，部门不会接受自己提供共享而对方不提供共享。若双方都不共享，虽然风险为零，但收益也为零。

因此，研究电子政务信息资源共享的安全保障机制对于推进电子政务信息资源共享建设意义重大，有效的安全机制能够降低共享带来的安全相关的风险。在随着共享程度提高而安全风险上升较慢的函数曲线存在的条件下，显然，“共享－共享”模式的共赢作用会逐步突出，政府机构间的共享效益和积极性也会相应提高，从而有效实现政府业务协同和信息资源共享。

2．共享与安全的平衡分析

共享与安全之间的平衡实质上是一种求最优解的问题。对于一个政务部门 A，设当前部门所掌握的信息量为 I_1，经过共享之后部门的信息增量为 I_2，总量为 I_3，概率 P_1 表示部门 A 在当前掌握信息量 I_1 的条件下，经过信息资源共享信息量为

I_3 的概率。则：

$$H_1=-\sum_{i=1}^{n}P_1(x_i)\log P_1(x_i)(n=1,2,\cdots) \tag{2-1}$$

其中，x_i 表示部门 A 信息集合中的元素，信息熵 H_1 描述共享信息的不确定性。

对于部门 A，设在当前部门所掌握的信息量 I_1 条件下政务成本、政务效率、服务质量（即收益）为 Q_1，经过共享之后部门的收益增量为 Q_2，总量为 Q_3，概率 P_2 表示部门 A 在当前收益 Q_1 的条件下，经过信息资源共享收益为 Q_3 的概率。则：

$$H_2=-\sum_{i=1}^{n}P_2(x_i)\log P_2(x_i)(n=1,2,\cdots) \tag{2-2}$$

其中，x_i 表示部门 A 收益集合中的元素，信息熵 H_2 描述共享信息带来收益的不确定性。

对于部门 A，设在当前部门所掌握的信息量 I_1 条件下信息安全风险为 R_1，经过共享之后部门的风险增量为 R_2，总量为 R_3，概率 P_3 表示部门 A 在当前风险 R_1 的条件下，经过信息资源共享风险为 R_3 的概率。则：

$$H_3=-\sum_{i=1}^{n}P_3(x_i)\log P_3(x_i)(n=1,2,\cdots) \tag{2-3}$$

其中，x_i 表示部门 A 信息安全风险集合中的元素，信息熵 H_3 描述共享信息带来信息安全风险的不确定性。

由于政务信息对国家安全和稳定的重要性，因此，共享与安全的平衡不是在共享信息不确定性 H_1 条件下，求最大 H_2 和最小 H_3 的最优问题，而是在共享信息不确定性 H_1 和共享信息收益不确定性 H_2 条件下，求解最小 H_3 的最优问题。

目标函数 $\min H_3$

约束条件 H_1

H_2

2.4.4　共享的原则

1．共享原则

信息管理学的共享原则包括贡献原则和防范原则两个方面。

（1）贡献原则

贡献原则又称“集约原则”，指信息管理者要善于最大限度地将组织拥有的信息，以及企业和组织成员拥有的信息贡献出来，供企业和组织及其全体成员使用。贡献原则是实现信息资源共享的前提。

（2）防范原则

因为信息是可以共享的，企业的竞争对手、敌对的国家等可以共享我们企业和国家的信息，由此产生了信息安全的问题，因而要求信息管理者随时予以防范，这就是信息管理的防范原则，也叫安全原则。

在电子政务信息资源共享中，一方面，为了提高我国电子政务信息化建设，政府管理部门倡导各个职能部门之间遵循“贡献原则”以加快电子政务信息资源共享建设；另一方面，为了保障政务信息安全，在电子政务信息资源共享中需要遵循“防范原则”以保证国家政务信息安全。

案例 3　北京市政务信息资源共享交换平台管理办法（试行）

第十三条　市级国家机关应当通过市共享交换平台的授权服务或本部门业务应用系统的授权功能，实施本部门对外共享政务信息资源的授权管理。

第十四条　通过市共享交换平台开展政务信息资源共享交换的需求方（以下简称需求方）和提供方（以下简称提供方）应当达成政务信息资源共享协议。提供方应当按照政务信息资源共享协议确定的共享内容、更新频率等，通过市共享交换平台及时对外共享政务信息资源。需求方应当按照政务信息资源共享协议的限定范围，使用通过市共享交换平台获取的政务信息资源，未经提供方允许不得共享给其他部门和个人。

第十五条　市共享交换平台实行信息安全等级保护制度，市共享交换平台目

录中心和交换中心安全保护等级为第三级。市级国家机关应当按照国家和本市信息安全等级保护相关规定进行目录节点和交换节点的安全定级，并根据要求配备相应的安全保障措施。各区、县信息化主管部门应当按照国家和本市信息安全等级保护相关规定进行区、县共享交换平台的安全定级，并根据要求配备相应的安全保障措施[76]。

案例 3 以制定政府管理办法的方式为应对信息资源共享中的安全问题做出了相关规定，体现了信息资源共享中的“防范原则”。

案例 4　广东省政务信息资源共享管理试行办法

第五条　政务信息资源共享遵循需求导向、统筹管理、无偿提供、保障安全的原则[77]。

案例 4 既涵盖了“贡献原则”，也体现了“防范原则”。

电子政务信息资源共享应强调把信息资源作为信息资产和战略资源来进行管理，以信息管理活动的标准化为基础，要能满足政务决策和各项业务活动的信息需要，能够有力地支持业务协同，同时应重视共享中的安全问题。

2．安全风险制约管理进步

当前信息化技术发展日新月异，各种新技术、新应用不断涌现。宽带、泛在、融合、安全的新一代信息网络发展演进不断加快，新一代移动通信、物联网、下一代互联网、大数据、云计算等方面的创新方兴未艾。Web 2.0 的出现，微博、社交网络的迅速发展，开拓了政府部门对于交互式社情民情收集和沟通的新渠道。随着第三代通信技术（3G）的推广普及和第四代通信技术（4G）的研发，高速度、宽频谱、智能化的特点将不断拓宽无线服务的应用领域，为电子政务建设提供了新的技术手段。技术的发展进步伴随着信息安全风险的提升，使得电子政务信息资源共享的管理难度增大。

[76] 资料来源[EB/OL]：http://www.syic.bjshy.gov.cn/xinxihfg/ShowArticle.asp?ArticleID=702。

[77] 资料来源：广东省经济和信息化委员会[EB/OL]. http://www.gdei.gov.cn/ flxx/dzzw/flfg/201005/t20100525_101018.html。

第 3 章
国内外电子政务信息资源共享的安全保障机制比较研究

3.1　国外电子政务信息资源共享的安全保障机制

3.1.1　加强领导和协调

在电子政务信息资源共享和信息安全建设中，世界发达国家和地区十分重视管理机构的设置、管理和协调，以强化对电子政务信息资源共享及信息安全工作

的领导，适应不断发展变化的电子政务和信息安全建设的需要。

1．美国

美国高度重视电子政务信息安全保障的领导和协调机制建设，成立了多个相关部门协调电子政务建设工作，并建立信息安全机构来推进各项信息系统保护计划的实施。

美国的电子政务工作由总统管理委员会直接领导，总统行政办公室与管理和预算办公室（OMB）两个部门联合执行。为实现总统关于加强电子政务建设的倡议，预算办公室组织成立了跨机构的电子政务特别工作组，以制定实施电子政务战略规划和保障电子政务信息安全。在 2002 年通过的《电子政府法》中规定：① 白宫管理和预算办公室下设一个电子政府信息办公室，由政府首席信息官（CIO）负责电子政府的资源协调和预算问题；② 设立一个由各个行政部门首席信息官组成的委员会，负责政府各部门的合作和信息资源共享。2009 年，奥巴马上台后签署首份总统备忘案《透明和开放的政府》。这个备忘录具体阐述了奥巴马的执政理念，他强调建立一个开放透明、公民参与、多方合作的政府。备忘录指出各行政部门和机构应利用新的工具、方法和系统，在各部门之间、各政府之间全面协作。

为了加强网络安全集中领导，2009 年 2 月，奥巴马政府设立国家网络安全顾问一职，负责制定政策，协调联邦机构力量，并直接向总统报告工作，网络安全顾问拥有审查联邦机构信息系统的安全性和关闭不安全的联邦机构信息系统的权力。2009 年 6 月，美国国防部长盖茨正式下令创建网络战司令部，以协调美军的网络安全以及指挥网络作战。网络战司令部作为美军网络战方面的最高管理机构，整合了各军种网络战资源，可以协调全军联合网络作战，提高了网络作战能力。2009 年 12 月，奥巴马任命了网络安全协调官员，负责领导白宫“网络安全办公室”，制定和发布国家信息安全政策，国土安全部、国家安全局、国防部、联邦调查局、中央情报局和国家标准技术研究院等机构负责具体执行。这些机构各司其职，相关公司及合作机构在保障网络空间安全工作中也发挥着重要的作用。

在信息安全管理体制建设方面，为了落实各项信息安全政策，美国将政策执行、监督、管理等权利分配给多个政府部门，构建了包括审计署、国家标准局、国土安全部、国防部和国土安全局等部门在内的信息安全管理体系，成立了“全国信息安全保障委员会”、“全国信息安全保障同盟”和“关键基础设施信息保障办公室”等 10 多个全国性机构。这些机构和部门为了解联邦政府信息安全状况和制定政策提供决策建议，并协调各项保护信息系统计划的实施。

在电子政务信息资源共享建设方面，美国注重法律与技术并重。

在技术方面，美国建立了由绩效参考模型、业务参考模型、服务参考模型、技术参考模型、数据参考模型构成的联邦组织框架（Federal Enterprise Architecture，FEA）。其中，数据参考模型由数据共享、数据描述和数据环境（Context）三个标准化域构成：数据共享定义为一个用户使用其他用户提供的信息资源；数据共享标准化域用“数据提供者-用户矩阵”来描述。数据描述标准化域提供了一个在数据结构（语法）和含义（语义）方面达成一致的方法，可以为数据发现、数据重用、数据共享、数据实体一致化、语义互操作提供支持。数据环境标准化域为数据提供与数据创建和使用有关的附加信息[78]。

在法律法规方面，美国国会早在 1966 年就颁布了《信息自由法》，以促进联邦政府信息公开，赋予公民更大的知情权。在随后的几十年中，这个法案被多次增补修订。1996 年，美国政府出台了《电子信息自由法增补案（*Electronic Freedom of Information Act Amendments*）》，法案要求所有的联邦信息都能够以电子版本的形式发布传播，并要求联邦部门设立电子阅读室，为公民获取电子信息提供便利。为促进信息公开，奥巴马政府建立了 recovery.gov 和 data.gov 两个网站，专门用于联邦政府的信息披露和数据公开[79]。data.gov 作为开放政府行动（Open Government Initiative）的旗舰级项目[80]于 2009 年 5 月 21 日启动，由联邦首席信息官委员会

[78] 金江军，韦政君．国外电子政务总体框架研究[J]．信息化研究，2008（6）：47-49.

[79] 姜雷，陈敬良．美国电子政务的立法现状及其对我国的启示[J]．北京工商大学学报（社会科学版），2011（3）：122-128.

[80] 《开放政府指令》（*Open Government Directive*）于 2009 年 1 月由美国总统奥巴马授权管理与预算办公室（OMB）发布。

（CIO Council）和 OMB 的电子政务与信息技术办公室负责建设，运维工作由总务管理局（GSA）承担[81]。

在电子政务信息资源共享战略制定方面，美国联邦政府特别重视信息的及时共享在各个部门联合反恐中的作用，并发布了美国情报部门信息资源共享战略[82]。2006 年 11 月，美国发布了《信息资源共享环境执行计划》，并在 2009 年完成了联邦政府信息资源共享的相关标准。针对联邦政府拥有的数据中心数目庞大、各机构之间共享困难的现状，美国于 2010 年 2 月 26 日发布了“联邦数据中心整合行动”，旨在减少能源消耗、优化空间利用率、改善 IT 资产的利用。同时，为解决美国联邦政府电子政务基础设施使用率低、资源需求分散、系统重复建设严重、工程建设难以管理以及建设周期过长等问题，2011 年 2 月 8 日，美国联邦政府 CIO 委员会颁布了联邦政府云战略。2012 年，奥巴马签署发布了《美国信息共享和保护战略》，明确将信息资源作为国家资产，并对联邦层面的信息共享，联邦与州、地方的信息共享等都提出了要求，制定了共享信息的机制、标准和制度。该报告提出，美国的国家安全依赖于在正确的时间与正确的人分享正确的信息。因此，将继续努力保证信息共享的方式是负责任的、无缝的和安全的，将继续利用关键信息资源来保卫国家安全、国民安全。

2．欧盟

欧盟在电子政务和信息安全保障建设的领导和协调方面表现为欧盟和各成员国两个层面规划建设并重。

（1）欧盟层面

在电子政务建设的领导机制方面，欧盟层面主要有五个决策机构：部长理事会、欧盟委员会、欧洲议会、欧洲理事会和欧洲法院。其中，欧洲理事会和部长理事会是政府间机构，是欧盟的主要立法机构；欧盟委员会和欧洲议会是超国家机构；欧洲法院是欧盟的最高法院，从司法角度保障欧盟的法律实施。按照《欧盟宪法条约》确立的“一体化”宗旨，欧盟注重发挥其领导协调作用，通过颁布

[81] 国家信息中心．电子政务发展前沿报告，2011（8）.

[82] GAO.United State Intelligent community Information Sharing Strategy, 2008: 2.

相关政策法规、召开各类专门会议及推广成功经验等多种措施，引导和督促成员国推进电子政务建设。欧盟委员会于 2010 年 12 月 15 日发布了《2011—2015 年电子政务行动方案》，提出到 2015 年可提供更加便利的社会保障和医疗福利网上申请程序。为加强电子政务安全建设，2004 年 3 月 10 日，欧洲议会和欧盟委员会颁布了《建立欧洲网络和信息安全机构的规则》，正式成立了欧洲网络与信息安全局（ENISA）。该机构建立的主要目的包括：① 加强欧共体各成员国和工商企业应对网络和信息安全问题的能力；② 在有关网络和信息安全方面向理事会和各成员国提供帮助和建议；③ 为公共部门与私人操作者之间的联系和合作提供便利条件，提高各成员国信息安全水平；④ 为欧盟理事会在网络和信息安全领域更新和发展欧共体法律提供技术准备和帮助。该机构的成立为欧盟各国电子政务信息资源共享的安全建设提供了大力支持。

（2）成员国层面

欧盟各成员国电子政务专职管理机构主要由领导机构、管理实施机构和协调机构三部分构成。其中，领导机构一般为内阁办公室或财政部，负责电子政务的研究规划和实施，在政治和财政上确保电子政府的建设；管理实施机构负责电子政务工作的具体实践；协调机构保证不同项目能够进行数据共享和跨平台建设。此外，欧盟各成员国的国家管理机构中都普遍设有信息局或信息技术局，负责审核下级电子政务建设规划，承担本级政府信息技术支持、管理工作。例如，法国政府设立了“电子与通讯技术局”、意大利政府成立了“技术革新部”、爱尔兰政府组建了“联络局”等来领导电子政务建设工作。2011 年 2 月，德国联邦政府通过了《德国网络安全战略》，成立“国家网络防御中心”，旨在通过综合利用多个政府部门的资源，促进各部门间合作，有效提高德国抵御潜在网络攻击的能力。

在电子政务信息资源共享建设方面，欧盟制定了一系列相关战略，主要表现为以下三方面的特点：

① 强调欧盟内信息资源共享，积极推动泛欧电子政务互操作。欧盟从国家层面入手，在共享机制方面采取了包括制定《欧洲互操作框架》、《欧洲公共服务互操作解决方案》等诸多行动，以加强成员国之间的交流合作，积极推动泛欧电子

政务的互操作性。这些战略和行动有助于实现在欧盟范围内公共机构、企业和公众的跨国境互动，真正提高欧盟电子政务的效率和效力。

② 注重交流和经验推广。欧盟委员会开通了推广优秀的电子政务建设经验的ePractice.eu网站，以促进欧盟各国电子政务建设发展。该网站中的“良好实践框架”项目为各成员国提供了一个电子政务信息交流和共享的平台，主要介绍电子政务的最佳实践，并将各国电子政务的最佳实践纳入该框架之中，供成员国进行交流和学习。

③ 强化合作。2000年欧盟推出的“E 欧洲行动计划”推动了欧盟各成员国政府部门间的信息交换和信息资源共享，欧盟成员国每启动一个新项目时都会考虑共享老项目的资源。

3．俄罗斯

在电子政务建设的领导和协调方面，俄罗斯政府成立了信息技术委员、参与信息通信技术研发及应用计划的跨部门委员会等部门以强化对电子政务建设的领导工作。在信息安全建设方面，俄罗斯对信息安全管理实行机构分工：俄罗斯安全委员会负责国家信息安全保密，俄罗斯科技委员会负责信息安全标准、评估和检验，俄通信信息部负责产业计划规划，俄联邦总统直属政府通信和信息局负责密码和通信安全，重大问题由联邦总统直接命令颁布执行。其中，俄联邦总统直属政府通信和信息局类似于美国的国家安全局（NSA），是集收集情报和信息安全两项职责于一身的重要机构。

在电子政务信息资源共享建设中，俄罗斯批准和颁布了一系列战略计划，其特点主要表现为以下几个方面：

① 重视信息资源共享。《2002—2010年俄罗斯信息化建设目标纲要》中提出，通过相关项目的建设实施各部门信息化建设，建立跨部门和地方性的信息系统和数据库，提高机构的工作效率。2008年，在信息通信技术日益广泛应用于国家权力机构及社会各领域的背景下，俄罗斯发布了首个官方电子政府战略性文件——《2010 年前俄罗斯联邦电子政府建设构想》（以下简称《构想》）。根据《构想》，俄罗斯将电子政府建设的目标设定为政府信息公开和提供国家服务。其中，在政

府信息资源共享方面提出：建立支持公民与国家机构间互动的统一的信息咨询系统、联邦互联网公共服务门户、联邦电话服务中心、部际数据交换网络、全俄罗斯国家信息中心等，确保各信息服务系统间的兼容性、互联性和实用性。

② 以法律法规推进信息资源共享和信息系统建设。在俄罗斯颁布的《2010 年前俄罗斯信息化发展联邦目标纲要》和开始实施的《电子俄罗斯联邦目标纲要》中，前者 68 个专项计划中有 24 项、后者 7 项措施中有 3 项直指电子政府建设。在“自动化=信息化=信息公开=行政效率”理念的指引下，俄罗斯政府又陆续出台了诸如《关于保障获取联邦政府及联邦执行机构信息的政府令》、《2010 年前联邦国家机构活动中信息技术应用构想》和《关于为国家及政府部门供应商品、实施工程及提供服务联邦法》等的后续政策，这些政策有力地推进了政府上网和信息系统建设工作的开展[83]。

③ 重视信息通信技术。俄罗斯开展了涉及联邦政府各部并由信息技术和通信部负责协调的核心 IT 计划——《2002－2010 年电子俄罗斯》，该计划为通过大规模推广信息和电信技术提高经济和政府管理效率打下了坚实基础。

4．日本

日本注重建立和完善电子政务的领导机制，成立了多个相关部门协调电子政务建设。在电子政务信息安全建设方面，日本先后成立了多个部门和机构强化对电子政务信息安全工作的领导和协调。

① 电子政务领导机制和相关部门设置。日本的电子政务建设由 IT 战略本部（首相兼任本部长）统一领导，IT 战略本部下设首席信息官联席会议具体负责协调电子政务建设。其中，首席信息官联席会议主席由内阁官房副长官担任，副主席则由总务省行政管理局局长担任，其成员为各省厅的首席信息官。首席信息官联席会议的日常事务由内阁官房在总务省行政管理局的辅助下处理。为了协助首席信息官开展工作，各省厅还设立了由首席信息官担任委员长的电子政务推进委员会。此外，日本还计划在各省厅设置首席信息官辅佐官，主要协助首席信息官及有关部门负责人完成业务和系统的分析、评估及制订最佳化计划等工作。

[83] 刘戈．俄罗斯电子政府发展思路分析[J]．电子政务，2010（5）：103．

② 信息安全建设的领导机制。为强化对电子政务信息安全工作的领导和协调，日本先后在总理府 IT 战略本部设立了网络信息安全促进室、网络信息安全促进调查会、网络信息安全基本问题委员会等机构。2005 年 4 月，在整合上述机构的基础上，日本总理府办公厅设立了网络信息安全中心（NISC），同年 5 月在日本总理府 IT 战略本部设立了网络信息安全政策委员会。此外，日本通过建立“ICT（Information and Communications Technology）构想恳谈会”，制定 ICT 新政来实现电子政务安全服务流程中应对防灾、减灾、实况报告标准化、灾情传递网络化、危机和突发事件处理信息化的目标。2009 年 1 月，日本政府批准了 2009—2011 年的第二个国家信息安全战略计划。这个三年计划包括四个主题：中央和地方政府、关键基础设施、商业团体、个人。作为国家信息安全战略计划的一部分，日本政府批准了“安全日本 2009”。在其 212 项政策中，1/4 针对改进中央和地方政府的职能；在关于关键基础设施和商业团体的部分，私人企业起行动主体的作用，而政府则提供支持。

在电子政务信息资源共享建设方面，日本政府 IT 战略总部于 2001 年 5 月 31 日发布的“e-Japan2002”计划在开发信息安全基础技术部分提出：在不泄密的前提下，向政府其他部门以及民间公开国防、治安方面的相关技术。另外，为了促进政务电子化创新和流程自动化创新，日本于 2009 年推出了《数字日本创新计划》。

5．韩国

联合国经济与社会事务部发布的 2010 年度全球电子政务调查报告（The 2010 United Nations e-Government Survey）显示，韩国的电子政务发展指数位居全球首位。截至 2010 年 12 月底，韩国 132 个中央和地方机构中，已经有 100 个机构应用了总体架构，应用普及率达到 75.8%[84]。《2014 年联合国电子政务调查报告（中文版）》显示，2014 年韩国的电子政务发展指数及其排名仍居全球首位。

在基础设施建设方面，韩国拥有世界上最发达的通信网络结构，232 个地方

[84] 王璟璇等．电子政务顶层设计：国外实践评述[J]．电子政务，2011（8）：13．

政府之间实现公民、交通等信息的完全共享[85]。2001 年，韩国成立了电子政务特别委员会（SCEG）以保障电子政务建设在各部门间的协作问题，同时成立了由著名专家和政府高级首脑组成的电子政务专门委员会来指导和规划电子政务建设。从立法层面看，韩国于 2005 年 12 月颁布了《政府信息系统有效采购和运作法》，作为指导信息系统规划和建设的法律；2009 年 5 月修订的《国家信息化法》规定各机构的首席信息官必须开发和使用总体架构，公共部门的电子政府工程也必须基于这一架构；2010 年 2 月《政府信息系统有效采购和运作法》被整合进修订后的《电子政府法》中，《电子政府法》明确规定所有的电子政务工程都应该基于政府企业架构[86]。

6．加拿大

在国际著名管理咨询公司埃森哲的全球电子政务发展年度报告中，加拿大连续多年被评为全球第一。加拿大电子政务的核心内容是“在线政府”（Government On-Line，GOL），这是一项让所有加拿大政府的服务对象通过电子方式与政府实现在线互动的计划。加拿大政府非常重视电子政务信息安全保障，1999 年年底，GOL 的监管、策略、隐私、安全、用户需求和获取等主要构成框架得以确立并初步建设成型；2002 年，提出“更佳的服务，更棒的政府”电子政务战略。

加拿大联邦政府（GC）在电子政务建设各阶段都提出了专门的信息安全计划，并就 PKI 的建设制定了一系列的发展规划和策略，以及相关的标准、法规。加拿大政府的 PKI 认证实现了不同安全级别之间的交叉认证，保证联邦机构能够在 Internet 和其他网络上安全地共享服务和规划。

在加拿大财政部中，CIOB 负责批准和颁布适合于信息技术安全的标准，这些标准的颁布主要是为了支持政府安全政策。CIOB 的基础设施、规划和安全部负责加拿大政府所承担的信息技术安全标准的协调工作。

[85] 陈姝宏．论韩国电子政务发展及对我国的启示[J]．东北亚研究，2009（4）：56-58.

[86] 中国电子政务网[EB/OL].[2013-01-04]. http://www.e-gov.org.cn/news/news004/2013-01-04/137406.html.

3.1.2 完善政策法规环境

1. 美国

（1）电子政务建设方面

美国颁布了一系列电子政务相关法规，用于指导电子政务建设，主要包括《政府文书销毁法》、《信息自由法》、《电子政府法》（*E-Government Act*）、《电子政府法实施指南》、《政府绩效结果法案》等（分类列举参见表 3-1）。经过几十年的不断完善，美国已经建立起相对完整的电子政务法律体系。其电子政务立法的特点突出表现为三个方面：一是美国的电子政务立法遵循渐进原则；二是美国的电子政务立法以技术进步为基本支撑；三是美国的电子政务立法与其机构调整及设立相辅相成。

表 3-1 美国主要电子政务法律法规的分类和列举

电子政务法规类型	法规政策举例
基础性	《电子政府法》、《电子政府法实施指南》、《联邦信息安全法》、《国家信息基础设施行动议案》
安全相关	《计算机保护法》、《网上电子安全法》、《反电子盗窃法》、《计算机欺诈及滥用法案》、《网络空间国家安全战略》
信息公开和个人信息保护	《公共信息准则》、《削减文书法》、《个人隐私保护法》、《儿童网络隐私保护法》、《信息自由法》、《电子隐私条例法案》
政府管理机制创新相关	《政府绩效结果法案》、《电子签名法》、《政府纸质文书消除法》、《信息技术管理改革法》

（2）信息安全建设方面

在制定信息安全相关的法律法规和战略方面，主要表现为以下几方面的特点：

① 起步较早，法律法规相对完善。早在 20 世纪 80 年代就已经开始针对美国关键基础设施和信息系统的脆弱性和漏洞，颁布了一系列有关信息安全的法律法规，包括《信息自由法》、《个人隐私法》、《反腐败行径法》、《伪造访问设备法》、《计算机安全法》、《正当通信法》、《电子签名法》、《反黑客法》等。

② 重视构建国家信息安全保障体系。1998 年颁布了《保护美国关键基础设施》，提出“最迟不晚于 2000 年，美国应当实现初步的信息安全保障能力”。1998 年年底，美国国家安全局制定了《信息保障技术框架》，为保护美国政府和工业界的信息与信息基础设施提供了技术指南。2008 年发布的《国家网络综合倡议》中，涉及可信因特网连接、入侵监测、入侵防范、网络反情报、强化涉密网安全、网络威慑战略和供应链安全等信息安全的多个方面。

③ 高度重视网络空间安全。2003 年出台的《网络空间安全国家战略计划》作为美国《本土安全战略》和《国家安全战略》的重要补充，是美国历史上第一份专门针对信息安全而推出的国家安全战略文本，标志着国家信息安全政策的独立地位得到了最终确认。2009 年 1 月奥巴马政府上台以后，依旧高度重视信息安全战略，积极主导了一个为期 60 天的信息安全评估项目，并公布了《美国网络安全评估》报告，评估了美国政府在网络空间的安全战略、策略和标准，试图改变美国信息安全保障不力的情况，着手制定新的国家信息安全战略。2011 年 5 月，白宫发布了《网络空间国际战略》，宣称将像对待其他任何威胁一样，使用一切必要手段对网络空间的敌对行为做出反应，并在多个领域出台了网络空间环境下的国家级安全战略。2014 年 2 月 12 日，奥巴马政府宣布网络安全框架正式发布，这是由关键基础设施私营部门主导的自愿性增强网络安全计划的工作之一。该框架是 2013 年美国政府发布的行政命令《提高关键基础设施网络安全框架》的核心成果之一。

④ 重视隐私保护。保护公民隐私是美国电子政府立法的一个主要要素。由于在日常工作中开始大量使用计算机对公民个人信息进行登记和匹配，美国国会于 1988 年增补了《隐私法》。新增补颁布的法案全称为《计算机匹配与隐私保护法》（*Computer Matching and Privacy Protection Act*）。该法案确定了联邦部门对公民个人信息进行登记匹配时所遵循的原则与程序，加强了对个人隐私的保护。同时，该法案要求所有进行信息登记和匹配的部门都要成立由资深行政官员组成的数据完整性委员会（Data Integrity Board），对整个匹配过程进行监督、评估，并定期汇报。

在信息安全标准方面，美国形成了较为全面的标准体系。美国信息安全标准的研究、制定和颁布主要涉及以下组织：以国家标准学会（ANSI）为代表的全国

自愿性标准体系管理和协调机构；以国家标准技术研究院（NIST）为代表的美国政府标准和技术研究机构；以美国国家安全局（NSA）为代表的美国军方标准化组织。另外，美国电气电子工程师学会（IEEE）、通信工业协会（TIA）、保险商实验室（UL）等数百个机构和部门，也是信息安全标准建设的重要力量。

① 美国国家标准主要包括：数据加密算法（ANSI X3.92-1981）、信息系统-数据链加密（ANSI X3.105-1983）、标识号的管理和安全（ANSI X9.8-1982）、公开密钥加密（ANSI X9.30-1993）、可信时间戳管理和管理（ANSI X9.95-2005）、信息技术-安全技术-信息安全管理系统要求（ANSI/INCITS/ISO/IEC 27001-2005）、信息技术设备安全第 1 部分：一般要求（ANSI/UL 60950-1-2006）等。

② 美国联邦标准（FIPS）主要包括：密码模块安全要求（FIPS 140-2，2001）、安全杂凑标准（SHS）（FIPS 180-3，2008）、数字签名标准（DSS）（FIPS 186-3，2009）、高级加密标准（AES）（FIPS 197，2001）、密钥散列消息鉴别码（HMAC）（FIPS 198-1，2008）等[87]。

③ 美国国防部指令（DODD）主要包括：信息安全保密程序（DODI 5200-1-1982 DOD）、国防可信计算机系统评估准则（DODI 5200.28-STD-1985）、计算机安全保密技术脆弱性报告程序（DODD 5215.2-1986）等。

2．欧盟

（1）电子政务建设方面

欧盟注重整体信息化推进、法制统一与充分发挥各国特长和优势互补的原则，从不同角度推进信息化发展和电子政务立法工作；利用欧洲一体化的优势，协调各国的法制环境，为电子政务创造无障碍的法制环境。欧盟在电子政务立法方面的突出特点表现为：一是注重合作性和包容性；二是重视信息安全和隐私保护。欧盟发布的具有法律效力的政策规定、法律法规、规划指令等主要包括：《电子签名指令》、《电子欧洲 2005 行动计划》、《公共部门采购指令》、《电子政府政策》、《i2010 战略》、《电子通讯法规框架》、《欧洲网络与信息安全机构设置规则》、《国家电子政府协同框架》、《网络安全议案》、《关于在信息高速公路上收集和传送个

[87] 杨晨，王慧莅，张明天，等．FIPS 信息安全标准研究[J]．信息技术与标准化，2011（4）：41．

人资料的保护》、《关于数据库法律保护的指令》、《个人数据保护指南》和《网络个人隐私保护的一般原则》等（分类列举参见表 3-2）。

表 3-2　欧盟主要电子政务法律法规

电子政务法规类型	法规政策举例
政策性文件	《关于实施对电信管制一揽子计划的第五份报告》、《电子通信服务的新框架》、《电子欧洲——一个面向全体欧洲人的信息社会》、《国家电子政府协同框架》
规范性和战略文件	《关于聚焦电信、媒体、信息技术内容及相关规范的绿皮书》、《欧洲共同体委员会信息社会的版权和有关权利的绿皮书》、《电子签名指令》、《关于电子欧洲 2005 行动计划第 2003/C48/02 号决议》、《公共部门采购的第 2004/18/EC 号指令》、《电子政府政策》、《i2010 战略》、《关于知识产权执法的第 2004/48/EC 号指令》、《电子通讯法规框架》
促进信息化发展相关	英国 2000 年的《电子通信法》、德国 1997 年的《信息与通信服务法》和《数字签名法》、意大利 1997 年的《数字签名法》和 2000 年的《电子信息与文书法》等
安全相关	《关于欧盟理事会制定确认、标明欧洲关键基础设施，并评估改善保护的必要性的指令的建议》、《欧洲网络与信息安全机构设置规则》、《网络安全议案》、《关于在信息高速公路上收集和传送个人资料的保护》、《关于数据库法律保护的指令》、《个人数据保护指南》、《网络个人隐私保护的一般原则》、《数据保存指令（2006/24/EC）》等

（2）信息安全建设方面

欧盟在信息安全建设方面的特点主要表现为：一是重视法律法规的建设；二是重视安全技术标准的制定，并积极参与开发国际通用安全准则。

欧盟在信息安全法律法规建设方面形成了一个多层次的法律体系，在法律法规制定中高度重视网络隐私权的保护，并积极关注安全新威胁，及时更新法律规范。

① 欧盟信息安全法律框架是由欧盟一体化立法、成员国立法、综合立法和专项立法构成的多层次法律体系，其结构、内容及实施措施等特点鲜明。欧盟信息安全的立法起点是 1992 年颁布的《信息系统安全领域框架决定》（92/242/EEC），此后欧盟陆续出台了《关于网络和信息安全领域通用方法和特殊行动的决议

（2002/C43/02）》、《关于对信息系统攻击的委员会框架决定（2005/222/JHA）》、《关于建立欧洲信息社会安全战略的决议（2007/C68/01）》，以及欧洲理事会《网络犯罪公约》等政策举措，有效地保证了整个欧盟的信息安全。1999 年 12 月 13 日，欧盟签署了著名的关于电子签名的 1999/93/EC 指令，并公布在 2000 年 1 月 19 日的公报上。

② 欧盟十分重视网络隐私权的保护，制定了四个对网络隐私权保护的框架文件：一是《关于电子通信行业个人数据处理与个人隐私保护的第 2002/58/EC 号指令》；二是为配合经济合作与发展组织的《关于隐私和个人资料的跨国境流动的保护指引》而制定的《关于在自动运行系统中个人资料保护公约》；三是欧盟委员会个人资料保护工作组制定的《关于向第三国传输个人数据的标准合同条款的委员会决定（2002/16/EC）》；四是部长会议关于互联网隐私保护指引备忘录中规定的《关于在信息高速公路上收集和传送个人资料的保护》[88]。

③ 欧盟重视应对新的安全威胁和风险的法律规范更新工作。例如，随着超宽带技术的发展，欧盟委员会于 2007 年 2 月 21 日颁布了允许在欧盟内部使用超宽带技术设备来利用射频频谱的第 2007/131/EC 号决定等。

欧盟十分重视安全技术标准的制定，并积极参与开发国际通用安全准则。2005 年，为适应互联网技术发展与新型在线技术的使用，欧洲议会和欧盟理事会先后出台了《关于制定技术标准和规章领域内信息供应程序的第 98/34/EC 号指令》、《关于制定促进更安全使用互联网和新型在线技术的共同体多年度计划的第 854/2005/EC 号决定》。自 2008 年 9 月以来，为应对互联网域名系统中的安全漏洞，提高网络的健壮性，以及推动先进、安全网络技术的普及，欧洲网络与信息安全局（ENISA）大力推广三种标准的技术——IPv6、域名系统安全扩展（DNSSec）和多协议标签交换（MPLS）。

3．俄罗斯

（1）电子政务建设方面

2010 年 11 月，俄罗斯总理普京签署了关于建立 2011—2020 年俄罗斯信息社

[88] 刘迎．欧盟信息安全保障框架概述[J]．信息网络安全，2009（8）：23-26.

会发展纲要，政府将每年拨款 1231 亿卢布用于实施信息社会建设项目。普京签署行政命令，要求俄罗斯联邦政府的各个部门在 2015 年前由私有软件转向免费或开源软件。俄经济发展与贸易部制定了《国家软件平台》计划，提出“保证在计算机信息技术领域的独立性，在一系列广泛的应用领域，使得软硬件的研制和生产达到国际先进水平[89]。”

在俄罗斯颁布的电子政务相关的法律法规方面，主要包括：《联邦信息、信息化和信息保护法》、《政府通信和信息联邦机构法》、《国家秘密法》、《信息保护设备认证法》、《俄罗斯联邦信息安全学说》、《关于保障获取联邦政府及联邦执行机构信息的政府令》、《电子签名法》和《关于为国家及政府部门供应商品、实施工程及提供服务联邦法》等（分类列举参见表 3-3）。

表 3-3　俄罗斯主要电子政务法律法规分类和列举

电子政务法规类型	法规政策举例
基础性	《政府通信和信息联邦机构法》、《国家秘密法》、《关于保障获取联邦政府及联邦执行机构信息的政府令》、《关于为国家及政府部门供应商品、实施工程及提供服务联邦法》、《2010 年前俄罗斯联邦电子政府建设构想》
安全相关	《信息保护设备认证法》、《俄罗斯联邦信息安全学说》、《电子签名法》
信息化相关	《联邦信息、信息化和信息保护法》

（2）信息安全建设方面

为确保电子政务信息安全，俄罗斯联邦政府联络和情报局为俄罗斯联邦国家政权机关建立了因特网网段 RGIN（Russian Government Internet Network），并在保障信息安全方面做了大量的工作：① 建成了高效安全的“阿特拉斯”数据传输，确保俄罗斯联邦各主体行政中心之间文件的网络传输，在最高国家机关安装了保障加密数据交换的技术设备，解决了该系统与国内其他通信网协同的技术课题；② 确立了《计算机系统安全评估标准》、《产品安全评估软件》等一系列完善的系统安全评估指标；③ 建立了联邦经济信息保护中心，负责政府网络及其他的专门网络、网络信息配套保护、国家政权机关信息技术保障等。

俄罗斯十分重视信息安全建设，从法令、机构、人员、资金、技术、管理等

[89] 杨国辉．2010—2011 年俄罗斯信息安全建设动态[J]．中国信息安全，2011（10）：71-72.

角度全方位地给信息安全工作予以支持和保障，发布了许多信息安全相关的法律法规，同时重视政务信息资源共享的安全保障问题。

在信息安全法律法规制定方面，俄罗斯 1994 年通过了信息安全保护法——《政府通信和信息联邦机构法》，通过宪法把信息安全纳入了国家安全管理范围。俄罗斯颁布的有关信息安全保护的法律和命令主要包括《产品和服务认证法》、《信息化和信息保护法》、《国家秘密法》、《参与国际信息交流法》、《信息保护设备认证法》、《有关遵守加密设备的研制、生产、实现和应用以及提供加密信息领域服务的合法性措施》、《俄罗斯联邦信息安全学说》、《俄罗斯信息社会发展战略》和《确保俄罗斯联邦信息安全的措施》等[90]。其中，《俄罗斯联邦信息安全学说》是官方对保障俄罗斯联邦信息安全的目的、任务、原则和主要内容的观点的总和，是制定和起草俄联邦有关安全保障的国家政策、法律、提案和专门计划的基础。在政务公开、信息资源共享的安全保障方面，俄罗斯在 20 世纪 90 年代就颁布了《联邦信息、信息化和信息保护法》，其中明确规定了在政务公开、信息资源共享等方面的安全保障问题和实施方案。

4．日本

（1）电子政务建设方面

日本重视电子政务法制环境的改善和政策能力的提升，通过立法引导并加强政府信息化建设，规范政府业务，并通过政府内外部管理和服务的规范化和示范化，加快公众对电子政务的接受。日本在电子政务相关的法律法规制定方面的突出特点表现在两个方面。一是紧密围绕 IT 技术。2000 年 11 月 29 日，日本制定了《高度信息通信网络社会基本法》，在这部法律中，推行行政的信息化改革是法定的重点改革之一。日本后续颁布和实施的电子政务相关法律法规如《U-Japan 政策》、《IT 新改革战略》中，都突出了 IT 技术在电子政务中的重要性。二是发布和制定具有连续性的电子政务发展战略。从《E-Japan 战略》到《E-Japan 战略 II》，到《IT 新改革战略》，到《数字日本创新计划》，再到《新 IT 战略案》，体现了日本在电子政务政策制定方面的连贯性（分类列举参见表 3-4）。

[90] 杨国辉．世界各国信息安全政策与策略[J]．中国信息安全，2010（11）：16-17.

表 3-4　日本主要电子政务法律法规的分类和列举

电子政务法规类型	法规政策举例
基础性	《高度信息通信网络社会基本法》、《U-Japan 政策》
安全相关	《个人信息保护法》、《确保电子政务实施过程中的信息安全行动法案》
战略相关	《IT 新改革战略》、《新 IT 战略案》、《E-Japan 战略》、《E-Japan 战略 II》、《数字日本创新计划》

（2）信息安全建设方面

日本在信息安全相关的法律法规制定方面，主要表现为以下特点：

① 重视网络和信息安全。例如，2000 年 11 月 29 日，日本颁布的《高速信息通信网络社会基本法》中明确规定，“在制定与高速信息通信网络社会形成相关的规定时，应当采取必要的措施，确保高速信息通信网络的安全性及可靠性，严密保护个人信息资料，使国民能够放心地利用互联网”（第 22 条）。2010 年 5 月 11 日，日本政府在信息安全政策会议上批准决定了“保护国民信息安全战略”，该战略提出了 2010—2013 年的具体努力项目与目标。

② 重视隐私保护。日本政府于 2000 年 9 月制定了《个人信息保护基本法大纲草案》，在涉及处理个人信息方面确定了限制利用目的、以正当方式获取、确保内容正确性、实施安全保护措施及确保透明性五个原则，并制定了违反相关政策法规的处罚原则。2001 年 3 月，《个人信息保护法》提交国会审议，2003 年 5 月经国会批准后付诸实施。

③ 重视电子政务安全建设。2001 年 10 月，日本公布了《确保电子政务实施过程中的信息安全行动法案》，该法案从信息安全政策、密码技术标准、信息监控机制、紧急应对机制等方面推动日本电子政务信息安全保障体系建设，促进信息资源共享。2013 年 5 月，日本发布“网络安全战略”最终草案，提出多项网络安全工作强化措施；同年，日本建立“信息安全政策会议”等机制，新设“内阁信息政策员”，负责统筹网络安全事宜[91]。

[91] 国家信息安全测评中心．2013 年度国家信息安全态势评估[M]．北京：时事出版社，2014：5-6．

5．韩国

在电子政务信息资源共享的安全保障建设方面，韩国较为突出的是强有力的法律法规和制度保障。韩国于 1996 年制定了《信息化促进基本法》；2000 年制定和修改了 107 项法案，包括《电子签名法令》、《个人情报保护条例》、《信息基础设施保护法规》、《数字内容管理条例》、《关于建立信息系统安全与保护个人信息隐私的条例》等；2001 年通过了《保护主要信息基础设施条例》；2005 年 12 月颁布了《政府信息系统有效采购和运作法》；2009 年 5 月修订了《国家信息化法》；2013 年 7 月公布了《国家网络安保综合对策》，加强国家信息安全领导协调[92]。韩国通过法律法规和制度建设，对电子政务的发展进行了清晰的责任界定，为电子政务信息资源的安全共享创造了较为完善的立法保障。

6．加拿大

加拿大注重完善电子政务信息安全保障的法规制度环境，先后颁布了《信息获取法》、《隐私法》、《个人信息保护和电子记录法》等。其中，《隐私法》对个人信息的收集、使用和处置都作了详细的规定。加拿大 TBS[93]于 2009 年 6 月 1 日推出的《文件保管指令》（*Directive on Recordkeeping*）强调有效的文件保管“是各部门能持续运作和提供服务，确保关键的部门职能能够满足问责、行业规范、评估、审计、信息获取、隐私保护、安全和政策服从的要求的基础”，并规定受此指令管辖的部委在 5 年内都要完成对它的执行[94]。

加拿大政府还发布了一系列与之相关的政策性文件（见表 3-5）。其中，经加

[92] 国家信息安全测评中心．2013 年度国家信息安全态势评估[M]．北京：时事出版社，2014：5．

[93] TBS 是 Treasure Board 的行政办公室，主要负责为 Treasure Board 制定的面向整个联邦政府的有关财务、人员、管理和职业道德等方面的政策、指示或条例出谋划策和监测这些政策、指令和条例的执行情况。Treasure Board 是枢密院的一个内阁委员会，由《财务管理法》（*Financial Administration Act*，FAA）设立，主要负责政府问责机制的执行，以及向各部委提供其工作所需的资源。根据 FAA，加拿大同时设置了财务部（Department of Finance），其主要责任包括除 FAA 赋予 Treasure Board 以外的职能，即与加拿大经济和金融有关的政策和法律的准备与制定，如财政预算、银行运行和税法修改等。

[94] 谢丽．互为促进的发展模式：加拿大联邦政府的电子政务建设与电子文件管理[J]．电子政务，2010（6）：42．

拿大财政部（Treasury Board）批准实施的《政府安全政策》（2002 年 2 月 1 日生效）指出，“在政府之间共享信息等资产时执行该安全政策并遵守相关的安全标准”、“对访问政府信息的个人必须进行安全审查，以确保其是可靠的、可信的”，以及“必须建立预防、侦查、响应和恢复等机制”等。另外，加拿大政府还出台了一些针对隐私保护的评估措施。

表 3-5　加拿大电子政务安全管理政策[95]

政策文件名	英文名称
《政府安全政策》	*Government Security Policy*
《信息安全法案操作标准》	*Operational Standard for the Security of lnformation Act*
《操作安全标准——业务连续性计划项目》	*Operational Security Standard—Business Continuity Planning Program*
《操作安全标准——信息技术安全管理》	*Operational Security Standard—Management of Information Technology Security*
《操作安全标准——物理安全》	*Operational Security Standard on Physical Security*
《操作安全标准——联邦政府设施准备水平》	*Operational Security Standard—Readiness Levels for Federal Government Facilities*
《职员安全标准》	*Personnel Security Standard*
《安全与合同管理标准》	*Security and Contracting Management Standard*
《安全组织与管理标准》	*Security Organization and Administration Standard*

3.1.3　强化保障措施

为推进电子政务信息资源共享和信息安全保障建设，世界各发达国家和地区制定了一系列战略计划，并开展了相关项目和工程建设。

1．美国

美国开展了一系列全国性的信息安全重大工程来推进电子政务安全建设，主要包括：实现对整个电子政务工程的安全控制的电子认证（E-Authentication）项目，

[95] 严明，刘琳．加拿大电子政务中的信息安全管理[J]．电子政务，2006（9）：24．

实现政务功能、信息资源共享和流程改造的 FEA（Federal Enterprise Architecture）项目，构建安全通信环境的无线公共安全通信计划（Project SAFECOM），等等。

此外，美国高度重视信息技术的研发和投入。① 重视网络安全技术研发。2009 年 2 月 1 日，美国白宫科技政策办公室发布的奥巴马总统关于 2011 年度财政预算案中提出，将向联邦通信委员会（Federal Communications Commission，FCC）和国土安全部（Department of Homeland Security，DHS）提供 250 万美元资金，以建立应急响应互操作中心（ERIC），确保公众无线宽带通信安全的可操作和互操作能力。2010 年 2 月 1 日，美国国家科学基金会（NSF）向国会提交了金额高达 74 亿美元的 2011 财年预算，2011 财年计算机信息科学与工程（CISE）学部将重点鼓励国家网络安全综合计划（Comprehensive National Cybersecurity Initiative，CNCI）等新兴优先领域的突破性研究，并对各种核心计算领域予以多方支持，其中 CNCI 的预算高达 5500 万美元。2010 年 3 月 16 日，美国联邦通信委员会（FCC）向国会提交了国家宽带计划（The National Broadband Plan），该计划致力于保护脆弱的宽带设施和数据传输免受网络威胁。② 重视隐私保护。奥巴马政府的 2011 财年预算提案其中一项为交通部项目 DOT（网络安全和隐私保护），该项目重点关注政府部门的网络安全和隐私控制，申请经费为 5400 万美元。

2．欧盟

为推进电子政务和信息安全保障建设，欧盟积极开展成员国之间的合作。2009 年 11 月 30 日，欧洲理事会就欧盟内部安全发布了信息管理战略结论，总结了欧洲理事会实施欧盟内部安全信息化管理战略的经验，拟定了未来要采取的行动。其中欧洲理事会决定采纳并执行信息管理战略，支持、简化并促进信息管理，确保欧盟内部的安全。2010 年 4 月，欧盟网络与信息安全局（ENISA）发布了 2010 年工作计划，包括三个“多年度专题计划”（Multi-annual Thematic Programs，MTP）和两项新的“筹备行动”（Preparatory Actions PAs）。三个多年度专题计划是：提高欧盟电子通信网络的弹性；建立和保持成员国间的合作关系；确定新兴风险以建立信任。两项新的筹备行动是：下一代互联网的身份识别、可审计性与信任；确定欧盟各部门网络信息安全合作的驱动力和框架。

在信息安全建设方面，欧盟制定了相关工作计划和项目研究，以信息安全建

设促电子政务发展。2005 年，各成员国的专家就“欧盟内部的身份管理”（Identity Management within the EU）项目展开了研究，以确定提高互操作性的电子身份（electronic Identification，eID）最佳方案，以便在尊重各国法律和文化差异的前提下，在欧盟范围内产生一个连贯的、清晰易懂的电子身份管理方案。同时，实施了跨国界安全身份认证（STORK）、泛欧洲公共采购网（PEPPOL）和跨境服务网上简易程序（SPOCS）大型试点项目。2010 年 4 月，欧盟网络与信息安全局（ENISA）发布了 2010 年工作计划，其中涉及“下一代互联网的身份识别、可审计性与信任”这一筹备行动，该筹备行动的总体目标是“确保欧洲在 ICT 基础设施和服务方面保持高水平的安全性，保持用户和企业的信心，同时减少对公民自由和隐私的威胁”。为实现此目标，ENISA 将研究与安全有关的电子服务模式，在这方面考虑采用对个人数据进行用户认可管理和废除的可用方法，将用户许可管理法扩展至多种环境，并评估这些方法在下一代互联网服务模式下的潜在应用。2010 年 11 月 4 日，欧洲首次举行全欧范围内的模拟网络战，目的是演练各国对付网络黑客攻击的能力。该演习是欧盟落实 2010 年 5 月制定的《欧洲数字议程》而采取的重要措施，议程要求加强网络安全，提高人们对网络的信任度。

3．俄罗斯

2010 年，俄罗斯政府信息技术委员会批准了俄罗斯通信部制定的关于实施建设“2011—2020 信息社会”长期方案的草案。该国家级项目的根本目的在于提高国民生活水平、改善商业环境、消除俄罗斯信息不对等问题、建立安全的信息社会、发展 ICT（Information Communication Technology）市场和保护文化遗产。其中提出，建立电子政府是建设信息社会中一项重要且紧迫的任务。政府信息技术委员会已批准在未来信息社会的建设框架下，正式实施俄罗斯通信部已制定一年之久的电子政府建设方案，此项方案是俄罗斯通信部系统地推进国家机关信息化进程的首次尝试。

4．日本

在发展战略方面，日本政府制定了多个信息安全和电子政务安全相关的战略和计划来指导其发展建设。

① 重视信息通信技术的发展更新。2009 年 7 月，日本发布了“i-Japan 战略

2015”计划，其中重点瞄准了下一代网络、下一代无线通信、信息安全等技术的研发。日本经济产业省发布的 2011 年度行动计划中提出要“加强公共领域的信息化与信息安全建设，完善信息安全政策”，其中包括整顿早期预警体制、防止机密信息因内部攻击而泄露、推广电子签名、开发可应对新威胁的技术等。

② 重视隐私保护。2010 年 3 月，日本内阁府 IT 战略总部公布了其拟制定的新的信息通信技术战略的要点，在“实现以国民为本的电子行政”中提到：“进行统计和调查时，应以保护回答者的个人隐私为原则，匿名采集信息，并保证这些信息能通过所有的互联网进行存取和使用。”同年 5 月 11 日，日本 IT 战略总部公布了《新 IT 战略案》，其中提出“充分利用 IT，推动电子行政服务”和“建立开放型网络行政”的具体措施。该战略中涉及电子政务安全方面的内容包括“于 2013 年年底前建立‘国民 ID 制度’，致力于实现国家与地方政府的数据交换，夯实国家和地方政府电子行政的‘共同基础’，支持国民对电子行政进行监督，加强个人信息保护”，以及“为了保护个人信息或隐私，应采取相应的保护措施，如以不暴露本人的形式匿名收集个人信息等”。这些都显示了日本政府在电子政务建设中对公民隐私信息安全的重视。

③ 重视网络安全。同在 2010 年 5 月 11 日，日本信息安全政策会议发布了根据会议议长——内阁官房长官的决定而制定的“第 2 次保护国民信息安全战略”，该战略的目标为：至 2020 年，克服用户使用网络和信息系统等信息通信技术的弱点，打造全体国民都能放心使用信息通信技术的环境（即：高质量、高可靠性、安全和放心的环境），把日本建成世界最尖端的信息安全先进国。

在加强国际合作方面，2010 年 5 月 11 日，日本信息安全政策会议发布了“保护国民信息安全战略”，其中重点提出要“从被动性的对策向主动性的对策转变，加强国际化合作”，包括加强与美国、亚洲和欧洲等国和地区的合作，以及加强与亚太经合组织、东盟地区论坛、国际电联等的合作等。

5．韩国

在电子政务信息资源共享的安全保障措施方面，韩国起步较早。20 世纪 80 年代中期至 20 世纪 90 年代中期，韩国政府重点投入建设的“国家基础信息系统（NBIS）”工程就涵盖了行政管理、财政金融、研究与教育、国防与国家安全等领

域（见图 3-1），为电子政务安全有效实施奠定了基础。

图 3-1　韩国“十年计划”（1987—1996 年）涵盖的五大领域

2001 年，韩国颁布了《电子政务法》，并设置了数额巨大的专项“信息技术促进基金”，从经济、制度两方面为电子政务的快速发展提供保障。

韩国最新的“2008—2012 电子政务计划”以“整合电子政务系统，提供无缝的公共服务”为目标，关键行动包括以下 4 个方面：① 以客户为中心的服务，加强公众参与；② 通过数字政府网络提供智能的行政服务；③ 实时的公共安全信息网络；④ 通过增强的隐私和安全，加强电子政务基础设施建设[96]。

6．加拿大

加拿大电子政务信息安全保障的重要特色是技术保障。加拿大“在线政府”（Government Online）采用“安全通道”（Secure Channel）接入服务方式，包括安全与认证服务，以保证政府在线交易的完整性和安全性；加拿大政府利用“e-Pass”项目来保证政府部门和机构的身份互认[97]。

加拿大政府十分重视对政府部门和机构各类人员的安全教育与培训。提供安全培训和教育的主要机构有财政委员会秘书处（Treasury Board Secretariat，TBS）、联邦安全员协会（Federal Association of Security Officials，FASO）、通信安全研究院（Communication Security Establishment，CSE）、关键基础设施保护与应急准备

[96] 姚国章. 韩国电子政务发展规划与电子政务发展最佳实践[J]. 电子政务，2009（12）：53-71.
[97] 姚国章，林萍. 加拿大电子政务发展规划与电子政务发展解析[J]. 电子政务，2009（12）：19.

办公室（Office of Critical Infrastructure Protection and Emergency Preparedness，OCIPEP）等，这些机构主要开展政策标准、安全意识、技术安全、人员安全、通信安全、风险评估等方面的教育和培训。

另外，加拿大还投入大量资金保证基础设施的安全，仅公共安全基础设施建设资金就占“政府在线行动计划”资金的 54%。

3.1.4 掌控新技术的发展创新方向

西方发达国家利用技术上的已有优势，推行对信息技术的垄断策略，把控核心设备、系统的研发，操纵技术标准、专利的制定，严防核心技术、源程序扩散，提出了再工业化、智慧地球、物联网、云计算等概念，把控核心信息技术的垄断地位，抢占未来发展的制高点。国际经济结构调整和生产方式变革不断加快，跨国公司利用全球生产和组织规模，谋求掌握全球价值链布局。

信息技术和产品的不断更新是通过不断创新来实现的。美国是通过创新得到迅速发展的典型例子，其建国之初模仿欧洲技术，后来走上了“只有创新才能超越”的高技术产业之路。美国正是沿着这条创新之路，登上世界信息技术及其产业化的顶峰，成为超级信息强国。自主创新是历史上和目前许多跨国公司普遍推崇的创新战略，也是跨国公司立足国际市场，保持和垄断竞争优势，不断发展壮大的重要战略之一。如垄断计算机软件的微软公司、主导计算机硬件的 IBM 公司、航空制造业巨头波音公司等，都是通过实施自主创新战略而享有竞争优势的。

在信息安全技术研发方面，美国在 2008 年就研制并实现了网络入侵探测体系并启动入侵探测计划，通过改进情报共享和计算机网络防御策略来对抗日益增长的网络战威胁。近期，美国陆军研究实验室和电子战联合公司合作开发的一种新的入侵探测体系旨在对抗高级持久的网络空间威胁。该体系是网络攻击特征描述和模拟试验台的一个组成部分，也是一种陆军研究实验室计算机网络防御系统，它通过提供对于新威胁做出迅速而灵活的感应来保护网络，以防敌人破坏。在云计算技术研究方面，美国政府正加大与大企业的合作力度，大力推进云计算平台的建设，试图通过对云计算平台的控制，更大范围地控制全球信息资源。

3.2　我国电子政务信息资源共享的安全保障机制

在国际发展的大环境下，信息技术突飞猛进，同时，在我国行政体制改革的内在驱动下，建立法制政府、服务型政府和效能政府是推动社会发展所必需的。自 20 世纪 90 年代后期开始，我国政府通过“政府上网工程”、“金字工程”等的建设，电子政务工作得到全面推进，为电子政务信息资源共享和安全保障体系建设创造了一个基础性的环境。具体表现在以下几个方面。

3.2.1　顶层设计

我国从 20 世纪 90 年代起就开始着手进行电子政务建设，尤其是在 1999 年“国家信息化领导小组”成立和“政府上网工程”启动后，国家有关部门出台了一些关键性的指导性意见。2013 年，中国信息化继续保持良好发展势头，网络空间与信息安全也取得了明显进展。以《关于加强网络信息保护的决定》全面实施为开端，到党的十八届三中全会上习近平总书记将网络与信息安全定位为“新的综合性挑战”，我国对信息安全的重视达到前所未有的高度，信息安全事业的发展迎来历史性机遇[98]。

1．国家政策

电子政务信息资源共享不仅仅是技术层面或业务层面的信息资源交互，更要求规划具有全局性的、集成化的电子政务信息体系架构。电子政务信息资源共享需要顶层设计，在我国电子政务信息资源共享发展的各个时期，针对各阶段所面临的问题和挑战，包括电子政务建设过程中的信息安全问题，国家出台了多个战略性文件和规划。

[98] 国家信息安全测评中心．2013 年度国家信息安全态势评估[M]．北京：时事出版社，2014：53．

（1）指导性文件

在我国电子政务信息资源共享的发展历程中有两个重要的指导性文件，分别为《国家信息化领导小组关于我国电子政务建设的指导意见》（中办发〔2002〕17 号文件）和《关于加强信息资源开发利用工作的若干意见》（中办发〔2004〕34 号文件）。

2002 年，中共中央办公厅、国务院办公厅联合下发的中办发〔2002〕17 号文件明确表示，要“把电子政务建设作为今后一个时期我国信息化工作的重点，政府先行，带动国民经济和社会发展信息化”。该文件指出，我国电子政务建设要坚持几项原则：一是统筹规划，加强领导；二是需求主导，突出重点；三是整合资源，拉动产业；四是统一标准，保障安全。当前要重点抓好建设统一网络平台、建立标准、健全法制，建设和整合关系国民经济与社会发展全局的业务系统。要正确处理发展与安全的关系，综合平衡成本和效益，一手抓电子政务建设，一手抓网络与信息安全，制定并完善电子政务网络与信息安全保障体系。

2004 年，中办发〔2004〕34 号文件指出“统筹协调”、“需求向导”、“创新开放”、“确保安全”是加强信息资源开发利用工作的主要原则。34 号文件在统筹协调方面指出，要“正确处理加速发展与保障安全、公开信息与保守秘密、开发利用与规范管理、重点突破与全面推进的关系”；在确保安全方面提出，要“增强全民信息安全意识，建立健全信息安全保障体系，加强领导，落实责任，综合运用法律、行政、经济和技术手段，强化信息安全管理，依法打击违法犯罪活动，维护国家安全和社会稳定”。紧接着，国信办发布了《国信办关于加强信息资源开发利用工作任务分工的通知》，明确了 34 号文件中各项重要工作的贯彻落实和任务分工，每项任务都具体到责任部门和负责落实的单位。

（2）总体框架

2006 年，国家信息化领导小组正式下发了《国家电子政务总体框架》（国信〔2006〕2 号）（以下简称《框架》），并为此专门召开了全国电子政务工作会议。文件提出了构建国家电子政务总体框架的要求：以邓小平理论和“三个代表”重要思想为指导，全面贯彻落实科学发展观，进一步发挥电子政务对加强经济调节、市场监管的作用，更加注重对改善社会管理、公共服务的作用，坚持政府主导与

社会参与相结合，坚持深化应用与提高产业技术水平相结合，坚持促进发展与保障信息安全相结合，保持政策的连续性与稳定性，统筹兼顾中央与地方需求，以提高应用水平为重点，以政务信息资源开发利用为主线，建立信息资源共享和业务协同机制，更好地促进行政管理体制改革，带动信息化发展，走中国特色的电子政务发展道路。《框架》提出了国家电子政务总体框架，包括：服务与应用系统、信息资源、基础设施、法律法规与标准化体系、管理体制。其中，基础设施是支撑，法律法规与标准化体系、管理体制是保障。《框架》还指出“要把信息安全基础设施建设与完善信息安全保障体系结合起来，按照‘谁主管谁负责，谁运行谁负责’的要求，明确信息安全责任”。

（3）中长期规划

“十五”以来，国家在电子政务的每个发展阶段都会提出中长期规划。我国政府在五年规划中将信息资源共享和安全保障的问题列为重要工作内容。《国民经济和社会发展第十个五年计划信息化重点专项规划》指出，信息资源开发、利用和共享是信息化发展的一个基本趋势，要通过有效的政策措施和法规，充分发挥市场机制的作用，加大信息资源开发的力度，促进信息资源的优化配置。《国民经济和社会发展信息化“十一五”规划》提出，要加快信息化法律、法规和标准体系建设，制定电信法、信息安全条例以及电子支付、个人信息保护、电子政务等方面的法律法规，适时修订和完善保守国家秘密法、消费者权益保护法及商用密码管理、电子证据等方面的法律法规。《国民经济和社会发展第十二个五年规划纲要》在“全面提高信息化水平”一章中明确指出，要“大力推进国家电子政务建设，推动重要政务信息系统互联互通、信息资源共享和业务协同”，以及“加强网络与信息安全保障”。

2005 年 11 月，国家信息化领导小组第五次会议通过的《2006—2020 年国家信息化发展战略》肯定了“十五”期间国家信息化领导小组在推行电子政务、加强信息安全保障等方面工作的全面部署和重要决策，指出“电子政务在提高行政效率、改善政府效能、扩大民主参与等方面的作用日益显著。信息安全的重要性与日俱增，成为各国面临的共同挑战”，强调“提升网络普及水平、信息资源开发利用水平和信息安全保障水平”是我国信息化发展的战略目标之一。表 3-6 列出

了我国电子政务信息资源共享进程中的问题与政策应对。

表 3-6　我国电子政务信息资源共享进程中的问题与政策应对

	问　　题	政　　策
“十五”时期	网络建设各自为政，重复建设，结构不合理；业务系统水平低，应用和服务领域窄；信息资源开发利用滞后，互联互通不畅，共享程度低；标准不统一，安全存在隐患，法制建设薄弱[99]	中共中央办公厅、国务院办公厅“关于转发《国家信息化领导小组关于我国电子政务建设的指导意见》的通知”（中办发〔2002〕17 号文件） 《关于加强信息资源开发利用工作的若干意见》（中办发〔2004〕34 号文件）
“十一五”时期	信息资源共享机制尚未建立；建设和应用发展不平衡，应用系统的潜能没有得到充分发挥，公共服务效率低；法律法规和标准化工作滞后，安全保障能力有待进一步提高；电子政务建设、管理、运行体制不完善，创新能力不强[100]	《国家电子政务总体框架》（国信〔2006〕2 号）
“十二五”时期	电子政务与政府职能转变的融合度不够；业务联动，资源整合难度大；部门管理功能强化，公共服务功能相对薄弱；电子政务推进机制依旧传统，未做到“部门的日常管理和服务融合起来一起推进”[101]	《中共中央关于制定国民经济和社会发展第十二个五年规划的建议》、《国民经济和社会发展第十二个五年规划纲要》

2．地方政策

在国家的指导和带动下，各级地方政府下发了配套文件，将电子政务信息资源共享和安全保障体系建设纳入地方发展规划，明确了电子政务信息资源共享建设目标。表 3-7 选取了部分省市的电子政务信息资源共享安全保障政策，并就主要内容作简要说明。

[99] 中共中央办公厅、国务院办公厅“关于转发《国家信息化领导小组关于我国电子政务建设的指导意见》的通知”（中办发〔2002〕17 号文件），2002.

[100]《国家电子政务总体框架》（国信〔2006〕2 号），2002.

[101] 电子政务“十二五”：面临的形势和任务[EB/OL].[2011-3-3].http://www.e-gov.org.cn.

表 3-7　主要省市电子政务信息资源共享安全保障政策

省（市）	文 件 名	相关内容
北京	《北京市国民经济和社会发展第十二个五年规划纲要》	“促进跨区域、跨部门信息资源共享与协作。” “创建信息安全可信城市。建设一流的安全测评、容灾备份、电子认证等城市信息安全基础设施。提高信息安全保障水平，重点加强公共网络、政务网络和无线电的信息安全建设。强化对信息网络、信息产品和网上交易行为的监管[102]”
天津	《中共天津市委关于“十二五”规划的建议》	“发展完善电子政务、电子商务、公共信息和云计算服务信息平台。加快城市应急指挥信息系统、空间地理信息系统、智能交通信息系统和社区管理信息系统等城市管理信息化建设。确保基础信息网络和重要信息系统安全”
上海	《中共上海市委关于制定上海市国民经济和社会发展第十二个五年规划的建议》	“加快推进以信息资源共享、系统集成为重点的电子政务建设，加大信息公开力度，加强重要信息系统建设，强化地理、人口、金融、交通和统计等基础信息资源开发利用，促进信息服务业发展。推进跨部门协同平台集成应用，建立集中与分布相结合的政务信息资源体系。以信息安全和资源共享为重点优化信息化发展环境。提高信息安全保障能力，加强信息安全保障体系建设，完善信息安全基础设施”
重庆	《重庆市国民经济和社会发展第十二个五年（2011—2015 年）规划纲要》	“统筹推进电子政务，建设全市统一互通的电子政务基础设施和内外网平台，构建集成民政、社保、税务、工商管理等公共服务的网络信息服务平台。建设面向全国及西部的数据交换中心、互联网数据中心、容灾备份中心，打造国家级信息资源集散地。强化网络信息安全保障体系，确保基础信息网络和重点信息系统安全”
宁夏	《宁夏回族自治区制定“十二五”期间规划的建议》	“以信息资源共享、互联互通为重点，加快全区政务网络建设，整合提升政府公共服务和管理能力”
西藏	《中共西藏自治区委员会关于制定“十二五”时期国民经济和社会发展规划的建议》	“着力提升信息化水平。加快基础电信网络、宽带通信、网络信息安全系统建设，建立应急通信系统，完善党政专用通信基础设施。基本建成覆盖区、地、县、乡四级的电子政务骨干传输网。推进信息骨干网络工程，加强进出藏干线光缆建设，推进边防覆盖和应急通信工程，建立党政专用网基础设施、电子政务、移动

[102] 北京市国民经济和社会发展第十二个五年规划纲要[EB/OL].http://www.bjpc.gov.cn/zt/shierwu/index.htm.

续表

省（市）	文 件 名	相关内容
西藏	《中共西藏自治区委员会关于制定“十二五”时期国民经济和社会发展规划的建议》	网广覆盖和宽带通信等信息化工程建设，推进“三网”融合，实现信息资源共享。建立健全基础设施维护和管理等机制，进一步改变重建设、轻管理的状况”
新疆	《新疆维吾尔自治区国民经济和社会发展“十二五”规划纲要》	“以基础信息网络和重要信息系统安全为重点，加强信息安全保障体系建设，基本完成自治区网络与信息安全保障体系建设，全面提高网络与信息安全防护能力，创建安全健康的网络环境。” “积极推进电子政务信息化，加快建设和完善全区统一的电子政务网络平台，初步建立形成以应用服务为目的的信息资源共享体系，加快自治区重点业务系统和应急指挥系统信息工程建设”
内蒙古	《内蒙古自治区“十二五”工业和信息化发展规划》	“推动跨行业、跨部门信息资源共享和业务协同。加强政务信息资源开发利用。继续完善各个重点业务系统建设。” “加强信息安全保障体系建设，提高网络和信息安全保障能力，确保基础信息网络和重要信息系统及信息内容安全可控。加强信息安全监控、预警预报、密码保障、网络信任、应急响应、容灾备份等信息安全基础设施建设”
黑龙江	《黑龙江省国民经济和社会发展第十二个五年规划纲要》	“统筹建设电子政务，推进电子政务网络互联互通和信息资源共享。强化人口、地理、金融等基础信息资源开发利用”
云南	《云南省国民经济和社会发展第十二个五年规划纲要》	“以信息资源共享、互联互通为重点，大力推进电子政务网络建设，整合提高政府公共服务和管理能力；提升网络与信息安全的保障能力和通信、邮政的普遍服务能力”
吉林	《吉林市国民经济和社会发展第十二个五年规划纲要》	“充分利用现有基础网络，建设全市标准统一、功能完善、互联互通、安全可靠的电子政务外网应用系统。加强地理、人口、金融、税收、统计等基础信息资源开发利用，建立健全城市规划、智能交通、应急指挥、环境监测等城市管理信息系统，加强国家规划的‘金字’业务系统和其他重要业务系统建设”
安徽	《安徽省国民经济和社会发展第十二个五年规划纲要》	“积极开展下一代信息基础设施建设，不断提高网络覆盖率和接入能力，提升信息安全保障水平。” “进一步推进电子政务网络建设，实现省、市、县（市、区）、乡镇（街道）联网，推动政府各部门实施网上协同办公，实现决策信息资源分层共享”

续表

省（市）	文 件 名	相关内容
山东	《山东省电子政务“十二五”发展规划》	“到 2015 年，覆盖全省统一的电子政务内、外网网络更加完善；政务信息资源公开和共享机制基本健全；目录体系与交换体系基本完善，重点相关领域之间资源共享与业务协同取得突破性进展；基础性、战略性政务信息数据库应用得到加强；信息安全保障体系、法律法规和标准化体系基本满足业务发展需求；电子政务服务逐步向乡镇（街道）、城乡社区（村）延伸，公众和社会对电子政务建设的满意度明显提高，电子政务应用水平走在全国前列”
山西	《中共山西省委关于制定国民经济和社会发展第十二个五年规划的建议》	“加快电子政务平台、网络建设，提升政府公共服务和管理能力。推动信息化和工业化深度融合，加快经济社会各领域信息化，重点推进城市管理、教育、医疗卫生、社会保障等方面的信息化应用和智能化水平。高度重视基础信息网络和重要信息系统安全”
广东	《广东省国民经济和社会发展第十二个五年规划纲要》	“加强各类信息网络的统筹规划、建设和管理，强化网络与信息安全保障，探索有效的共建共享机制。” “完善信息安全标准体系和认证认可体系，加强信息网络监测、管控能力建设”
广西壮族自治区	《广西壮族自治区国民经济和社会发展第十二个五年规划纲要》	“加强信息网络监督、管控能力和无线电频谱监管设施建设，确保信息网络系统安全。监控建设电子政务网络和基础数据库，实现重要政务信息系统互联互通、信息资源共享和业务协同”
江苏	《中共江苏省委关于制定江苏省国民经济和社会发展第十二个五年规划的建议》	“以信息资源共享和互联互通为重点，大力推进电子政务网络和信息公共服务平台建设，加强网络信任体系和安全设施建设，确保基础信息网络和重要信息系统安全[103]”
江西	《江西省国民经济和社会发展第十二个五年规划纲要》	“突破区域、部门、行业界限，合理布局传输通道，整合资源，加快信息通信基础网络建设，加强信息通信安全保障，大力推进电子政务、电子商务和物联网的发展，推动经济社会信息化”
河北	《河北省国民经济和社会发展第十二个五年规划纲要》	“……构建宽带、融合、安全的新一代信息基础设施。” “建设完善网络信息安全保障体系。健全和完善信息安全管理体系、信息安全应急处置体系和通报机制，加强网络与信息安全技术手段和力量建设。强化党政机关互联网安全接入，建立网络信任体系，提高安全保障能力”

[103] 中共江苏省委关于制定江苏省国民经济和社会发展第十二个五年规划的建议[EB/OL]. http://theory.people.com.cn/GB/13269986.html [2011-10-20].

续表

省（市）	文 件 名	相关内容
河南	《河南省国民经济和社会发展第十二个五年规划纲要》	“促进网络资源共享和互联互通，健全信息安全保障体系”，包括提高基础信息网络业务承载能力、加快建设重大应用网络平台、大力推动重大信息系统建设、健全网络信息安全保障体系
浙江	《浙江省国民经济和社会发展第十二个五年（2011—2015 年）规划纲要》	“完善信息基础设施，……发展电子商务和电子政务。” “加快空间信息基础设施建设……建成浙江省地理空间数据交换和共享平台”
海南	《海南省国民经济和社会发展第十二个五年（2011—2015 年）规划纲要》	“整合现有政务网络资源，建设统一的电子政务网络，建立协同办公、资源共享、科学管理的运行机制，提高电子政务应用水平”
湖北	《湖北省国民经济和社会发展第十二个五年规划纲要》	“加快信息基础设施建设，努力提高信息技术的公共服务能力与应用水平，建设“数字湖北”和“智慧武汉”，基本建成覆盖全省、多网融合、安全可靠的综合信息基础设施。” “完善基础信息资源目录体系和交换体系，实现基础数据的整合与共享。加强信息安全预警和应急处理，实行重要信息系统和安全保密设施同步规划、同步建设、同步使用，保障基础信息网络和重要信息系统安全，全面提高信息安全防护能力”
湖南	《湖南省国民经济和社会发展“十二五”规划纲要》	“加强重点领域信息化应用，加强人口、法人、自然资源、空间地理等公共基础数据库建设与应用，促进部门资源共享与业务协同。” “强化网络信息安全保障，深化信息安全等级保护和风险评估，建立网络与信息安全事件应急防范综合支撑平台，增强网络信息监测、预警和管控能力，提高重要信息系统的容侵、容灾和抗毁能力”
甘肃	《甘肃省国民经济和社会发展第十二个五年规划纲要》	“继续推进电子政务，优化整合网络资源，加强信息资源的公益性开发和服务”
福建	《福建省国民经济和社会发展第十二个五年规划纲要》	“完善全省政务信息网，完善提升“金字工程”，建设应急指挥体系……加强地理、人口、金融、税收、统计等基础信息资源开发利用。加强网络信息安全保障体系建设，确保基础信息网络和重点信息系统安全”

续表

省（市）	文 件 名	相关内容
四川	《四川省国民经济和社会发展第十二个五年规划纲要》	“大力发展电子政务，推动资源共享和业务协同，加强地理、人口、金融、税收、医疗、社保、就业、统计等信息系统建设，推进社会公共服务信息化。加强电子政务运行维护体系建设，基本实现电子政务建设和运行维护的制度化、规范化和专业化” “建立健全信息安全保障体系、应急通信体系，建设数据灾备中心，强化网络保密体系，加强信息网络监测、管控能力建设，实施信息安全等级保护和风险评估制度，加强信息网络、信息内容安全保障和技术防范，确保基础信息网络和重要信息系统安全”
贵州	《贵州省铜仁地区国民经济和社会发展第十二个五年规划纲要》	“整合现有专业网络，建设全区标准统一、功能完善、互联互通、安全可靠的电子政务网络平台。” “实施信息安全等级保护制度，构建全社会信息安全保障体系。” “推进信息资源的有效整合。开发和整合信息资源，实现信息资源共享”
辽宁	《辽宁省国民经济和社会发展第十二个五年规划纲要》	“继续推进文化信息资源共享……” “加强平安城市、企业生产监控等重点领域信息平台和网络建设，确保基础信息网络及重要信息平台和网络安全”
陕西	《陕西省国民经济和社会发展第十二个五年规划纲要》	“全面落实信息安全等级保护、涉密信息系统分级保护和风险评估制度，加强信息安全基础性工作，强化网络安全管理，保障基础信息网络和重要信息系统安全。加强以密码技术为基础的信息安全防护和网络信任体系建设，建立网络和信息安全监控、应急响应和容灾备份体系，完善保障网络和信息安全的长效机制”
青海	《青海省国民经济和社会发展第十二个五年规划纲要》	“构建宽带、泛在、融合、安全的下一代信息基础设施，推动信息化与工业化深度融合，加快党政信息系统和基层综合信息平台建设……确保基础信息网络和重要信息系统安全。” “加快‘数字青海’进程，强化地理、人口、金融、税收、统计等基础信息资源开发。” “以完善设施、信息资源共享、互联互通为重点，加快建设覆盖省、州（市、地）、县、乡的电子政务内外网，实现政务信息资源共享和业务协同”

3.2.2 政策法规

1. 法律法规

我国从电子政务起步阶段开始，颁布了一些与计算机网络有关的条例，如1991 年通过的《计算机软件保护条例》、1994 年国务院颁布的第一部关于计算机信息安全的法规《中华人民共和国计算机信息系统安全保护条例》，接着相关部门和地方政府的电子政务立法活动也活跃起来。但总的来说，我国现有的电子政务法律法规大多分散在计算机法、信息法、互联网法等单行法中，且大多是部门立法和规章，法律效力层次较低，缺乏统一的、纲领性的立法及明确的立法原则和标准，冲突现象严重。因此，我国尚未构建起有关电子政务的完整法律体系，在很多问题上的立法空白制约了我国电子政务的正常发展。

目前，我国信息网络安全立法体系框架分为四个层面，分别为法律、行政法规、地方性法规和规章及规范性文件。

（1）法律

《中华人民共和国电子签名法》是我国信息化领域的第一部法律，它规范了电子签名行为，确立了电子签名的法律效力，规定了合法的电子签名应具备真实性和可靠性。配套《电子签名法》实施的《电子认证服务管理办法》规范了电子认证服务行为，对电子认证服务提供者实施监督管理。2011 年 6 月，工业和信息化部（以下简称“工信部”）信息安全协调司对《电子签名法》颁布实施后的第一个规划——《电子签名与认证服务业“十二五”发展规划（讨论稿）》开展了意见征求会，对于政府机关和服务机构形成合力共同推动电子签名与认证服务业健康有序发展具有重要作用。另一项信息安全领域的典型法律是《中华人民共和国保守国家秘密法》，它明确了国家秘密的范围、保密制度、监管和法律责任。其他如《宪法》、《刑法》、《治安管理处罚条例》、《国家安全法》、《全国人大常委会关于维护互联网安全的决定》等也对信息安全保障做出了相应的规定。刑法修正案（七）增加了信息安全保护条款，加大了对侵犯公民个人信息和网络违法犯罪行为的处罚力度。2011 年 6 月，最高人民法院、最高人民检察院联合发布了《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》于 2011 年 9 月 1 日起

施行，对于依法惩治危害计算机信息系统的犯罪活动，维护正常的计算机网络运行秩序，具有重要意义。

稳步推进信息安全立法工作。2012 年 7 月 17 日，国务院下发了《关于大力推进信息化发展和切实保障信息安全的若干意见》，对保障信息安全工作提出了明确要求：要加强统筹协调和顶层设计，健全信息安全保障体系，切实增强信息安全保障能力，维护国家信息安全，促进经济平稳较快发展和社会和谐稳定；并提出了健全安全防护和管理、加快安全能力建设等重点工作。2012 年 12 月 28 日，全国人大常委会通过了《关于加强网络信息保护的决定》，《决定》强调了以法律的形式保护公民个人及法人信息安全，确立了网络身份管理制度，明确网络服务提供者的义务和责任，并赋予政府主管部门必要的监管手段，重点解决了我国网络信息安全立法滞后的问题[104]。2015 年 7 月 7 日，我国《网络安全法（草案）》出台，加强维护网络空间主权和国家安全、社会公共利益，保障国家网络安全。近年来，中央政府、各地方政府和各重要行业持续推进信息安全风险评估工作。

（2）行政法规

我国与信息网络安全有关的行政法规主要有：《中华人民共和国计算机信息系统安全保护条例》（国务院令 147 号）、《中华人民共和国计算机信息网络国际联网管理暂行规定》（国务院令 195 号）、《计算机信息网络国际联网安全保护管理办法》（公安部令 33 号）、《商用密码管理条例》（国务院令 273 号）、《计算机软件保护条例》（国务院令 339 号）、《中华人民共和国认证认可条例》（国务院令 390 号）、《计算机病毒防治管理办法》（公安部）、《关于加强互联网域名系统安全保障工作的通知》（工信部）、《通信网络安全防护管理办法》（工信部）等。其中，公安部公布的《计算机信息网络国际联网安全保护管理办法》中规定了任何单位和个人不得利用国际互联网制作、复制、查阅和传播有害信息。

（3）地方性法规

结合国家信息安全保障的政策要求，许多省市也出台了信息安全管理办法或

[104] 国家信息中心，中国信息协会. 2013 中国信息年鉴[J]. 北京：中国信息年鉴期刊社，2013：40-43.

规定，如《四川省计算机信息系统安全保护管理办法》（1996-03-28）、《黑龙江省计算机信息系统安全管理规定》（1997-08-05）、《北京市计算机信息系统病毒预防和控制办法》（1997-12-21）、《北京市党政机关计算机网络与信息安全管理办法》（2001-11-15）、《广东省计算机信息系统安全保护条例》（2007-12）等。

（4）其他

除了与信息安全直接相关的法律法规，其他一些法律法规也关注或更新了信息安全保障方面的内容，尤其是民法中对信息网络时代个人权益的保护。如在个人信息安全方面，2011 年 7 月起施行的《中华人民共和国社会保险法》对泄露个人信息的行为做出了处罚规定；在网络用户利益保护方面，2010 年 7 月起实施的《中华人民共和国侵权责任法》明确规定，网络用户侵害他人的民事权益将承担侵权责任。2011 年 10 月 24 日，全国人大常委会审议居民身份证法修正案草案，规定“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员泄露在履行职责或者提供服务过程中获得的公民个人信息，构成犯罪的，依法追究刑事责任”。

2．等级保护工作

信息安全等级保护是国家在国民经济和社会信息化发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化健康发展的基本制度。2004 年 7 月 3 日，国家网络与信息安全协调小组第三次会议审议通过了《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66 号，以下简称“66 号文件”），明确了公安机关负责全国信息安全等级保护工作的监督、检查和指导工作。国务院信息化工作办公室也发布了《电子政务信息安全等级保护实施指南（试行）》（国信办〔2005〕25 号），用于指导电子政务建设中的信息安全等级保护工作。

在具体实施方面，公安部根据《中华人民共和国计算机信息系统安全保护条例》等国家有关法律法规，制定了《信息安全等级保护管理办法（试行）》。国家信息安全等级保护工作协调小组办公室汇总发布了《全国信息安全等级保护测评机构推荐目录》，已向社会公布了 54 家测评机构，其中国家级的测评机构 5 家，计划年内向社会公布的测评机构达到 100 家。公安部会同国资委出台了《关于进

一步推进中央企业信息安全等级保护工作的通知》，央企等级保护工作将全面展开。此外，公安部建立了 54 个部委参加的中央国家机关信息安全等级保护联络员机制，并于 2011 年 4 月 7 日召开了联络员机制成立大会。

在宣传方面，公安部组织拍摄了等级保护工作宣传片及教学片，发各部委、各省市，并在 2011 年 3 月 7 日召开了发布会。另外，相关机构还举办了全国信息安全等级测评师培训班，推选全国信息安全等级保护测评机构等活动。

等级保护工作在我国电子政务系统得到了很好的推广应用。公安部、国家保密局、国家密码管理局、国务院信息化工作办公室于 2005 年年底发布了《关于开展信息安全等级保护试点工作的通知》，于 2006 年年初在北京、山西、上海、江苏、浙江、安徽、江西、山东、河南、湖北、广东、广西、重庆等 13 个省开展了试点工作，取得了较好的成绩。

此外，我国积极开展定级工作。2007 年 7 月 16 日，公安部、国家保密局、国家密码管理局、国务院信息办联合出台了《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔2007〕861 号）。2007 年 7 月 20 日，四部委在北京联合召开了“全国重要信息系统安全等级保护定级工作电视电话会议”，部署在全国范围内开展重要信息系统安全等级保护定级工作。

3.2.3　信息安全基础设施建设

中办发〔2002〕17 号文件明确指出，要“组织建立我国电子政务网络与信息安全保障体系框架，逐步完善安全管理体制，建立电子政务信任体系，加强关键性安全技术产品的研究和开发，建立应急支援中心和数据灾难备份基础设施”。《关于加强信息资源开发利用工作的若干意见》（中办发〔2004〕34 号文件）指出，加强信息资源开发利用工作的主要原则之一是“确保安全”，要“增强全民信息安全意识，建立健全信息安全保障体系，加强领导，落实责任，综合运用法律、行政、经济和技术手段，强化信息安全管理，依法打击违法犯罪活动，维护国家安全和社会稳定”。

在信息安全技术基础设施建设方面，《国家电子政务总体框架》指出，要“围绕深化应用的需要，加强和规范电子政务网络信任体系建设，建立有效的身份认证、授权管理和责任认定机制。建立健全信息安全监测系统，提高对网络攻击、病毒入侵的防范能力和网络失泄密的检查发现能力。统筹规划电子政务应急响应与灾难备份建设。完善密钥管理基础设施，充分利用密码、访问控制等技术保护电子政务安全，促进应用系统的互联互通和信息资源共享”。

1．网络信任体系

网络信任体系是国家信息安全保障体系建设的重要内容。我国网络信任体系建设主要以密码技术为基础，以法律法规、技术标准和基础设施为主要内容，用于解决网络系统的身份认证、授权管理和责任认定等问题。身份认证在网络环境中确认用户的身份，提供了网络行为主体的真实性；授权管理是对网络中各种行为主体访问、利用、处理信息资源而进行管理的重要手段；责任认定是实现网络行为可核查、网络事件责任可追究的技术基础[105]。

在电子政务信息资源共享中，网络信任体系就是要帮助用户对电子政务信息资源安全共享建立信心，并且为政务信息资源共享提供规避风险的手段。电子认证工作是我国网络信任体系建设的重点，2006 年 2 月发布的《关于网络信任体系建设的若干意见》（国办发〔2006〕11 号文件）对规范和加强电子认证工作做出了重要部署。在身份认证管理和应用方面，当前我国行业和区域性 CA 发展很快，电子认证服务机构规模逐步扩大。自 2005 年 2 月 8 日原信息产业部依法制定并发布了《电子认证服务管理办法》（2005 年 4 月 1 日起施行）后，工信部对企业开展电子认证服务资质审核和许可证的颁发，电子认证服务机构负责发放 CA 证书。2010 年，国家发展和改革委员会（以下简称“发政委”）批准成立“国家电子政务外网管理中心电子认证办公室”，主要负责电子政务外网数字证书认证业务的相关管理、运行和服务工作，其中电子认证服务工作由国家电子政务外网数字证书中心承担。截至 2015 年 12 月 31 日，全国有效电子认证证书持有量合计 320 001 012 张，其中机构证书 31 251 291 张，个人证书 285 853 165 张，设备证书 2 896 556

[105] 任金强，吴亚非，罗红斌等．国家电子政务外网网络信任体系的设计与实践[J]．电子政务，2008（6）：27-30．

张，应用于电子商务和电子政务中面向社会公众服务的各个领域。网络信任体系的授权管理和责任认定目前主要通过业务系统的功能来实现，涉及访问控制、安全审计等技术。

网络信任体系的技术基础是公钥基础设施（PKI）、授权管理基础设施（PMI）和审计技术等。目前我国发布了一些技术标准，主要有《信息安全技术 公钥基础设施 PKI 系统安全等级保护评估准则》、《信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求》、《信息安全技术 公钥基础设施 签名生成应用程序的安全要求》、《信息安全技术 公钥基础设施 电子签名卡应用接口基本要求》、《信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范》等，在已公布的信息安全技术标准中，有关网络信任体系建设的标准占有较大比例。

2．监控体系

网络监控系统是具备较强信息处理能力的信息监控系统，用于对重要信息系统抵御网络攻击、防范失窃等提供支持。电子政务信息安全监控体系能够对政务网络和重要信息系统的安全事件进行实时监控和预警，确保信息安全事件能够在第一时间知晓，并能够通过及时采取措施避免酿成重大安全事故。

从目前来看，尽管我国尚未建成全国性的信息安全监控体系，但可喜的是，一些地方和行业的监控体系建设已卓有成效。例如，北京市从 2005 年开始开展政务信息安全监控工作，目前已建成较为完整的政务信息安全监控体系，具备监控网络攻击、木马病毒传播、网站安全性、异常行为，检测僵尸网络和分析海量数据等能力，初步实现了对市政务网络和重要信息系统的安全事件的实时监控和预警，初步实现了能够实现对市政务网络和重要信息系统的安全事件实时监控、预警能力，监控范围覆盖了市政务外网汇聚节点、市重要政务网站、重要信息系统和市级重要政务用户互联网接入点，全市共有 67 个监控节点 300 余台（套）设备。市政务信息安全监控实行平时 7×8 小时、重大活动期间 7×24 小时的值守机制，日均分析安全报警约 12 万次，每年发现并处置安全事件 100 余起，出色地完成了第 29 届奥运会、中非合作论坛、国庆 60 周年等多项重大活动期间的信息安全保障任务。2011 年 6 月 30 日，北京市政务信息安全监控预警系统正式投入运行，

并于 2015 年 4 月开始进行升级改造[106]。自 2002 年起，国家广播电影电视总局利用相关技术，搭建了较为完善的播出前节目审核、播出后节目监控体系，较好地落实了“安全播出”的任务。湖北通信管理局注重在推进三网融合的进程中做好信息安全监控，成立了行业协调小组，制定了网络与信息安全监控方案。

3．灾备体系

电子政务系统中承载的信息包括机密信息和业务敏感信息，如果由于系统故障和未能预期的灾难造成电子政务系统崩溃或停止运行，将会给政府和公民造成重大的损失。灾难备份是确保电子政务系统在社会紧急状态下仍能保证其主要业务健康运行的有效手段，成为电子政务信息安全保障体系建设的重要内容。

我国的灾备市场虽然起步较晚，但发展迅速，同时随着云计算和虚拟化技术的发展，灾备市场将实现新的突破。在中办发〔2002〕17 号和中办发〔2003〕27 号等重要文件中，都提出了“建设灾难恢复中心”和“建立应急支援中心和数据灾难备份基础设施”的要求。灾难恢复是将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态而设计的活动和流程。2005 年国信办《重要信息系统灾难恢复规划指南》和 2007 年国家标准《信息安全技术 信息系统灾难恢复规范》（GB/T 20988—2007）发布后，越来越多的部门和企业意识到信息系统灾难备份与恢复的重要性。2010 年 7 月，工信部表示我国将制定强制性灾备建设规范，及时出台灾难恢复服务资质管理办法，促进政府相关部门、行业用户、企业灾难恢复保障体系的发展。同时，金融、保险、证券等灾难备份重点行业也制定了灾备标准。如 2008 年 2 月中国人民银行发布实施了《银行业信息系统灾难恢复管理规范》（JR/T 0044—2008），2008 年 3 月保监会发布了《保险业信息系统灾难恢复管理指引》，2009 年中国证券业协会发布了《证券公司网上证券信息系统技术指引》等文件，都强调了信息系统灾难恢复、应急预案和应急演练的重要性。

[106] 北京信息安全服务平台．北京市政务信息安全监控预警系统正式投入运行[EB/OL]. http://www.bjtec.org.cn/cenep/html/00000000000000001264/120010/article_show_b467505121a143fd86393fc8f4493ffc.html.[2016-02-27].

4．应急响应体系

应急响应体系是为了应对信息安全突发事件而建立的信息网络安全保障体系，包括检测、抵御、恢复、跟踪等环节。“确保恢复”和“追究责任”是应急响应体系的两大根本任务，即确保受影响的系统恢复正常功能，以及展开调查分析追究事件的原因。我国在建立信息安全应急响应体系方面着手较早，在组织建设信息安全应急响应体系方面做了很多工作。1999 年 5 月，清华大学信息网络工程研究中心成立了我国第一个专门从事网络安全应急响应的组织——中国教育和科研计算机网络安全应急响应组（CCERT）。2001 年，成立了在信息产业部互联网应急处理协调办公室的直接领导下的国家计算机网络应急技术处理协调中心（CNCERT/CC），负责协调我国各计算机网络安全事件应急小组（CERT），共同处理国家公共互联网上的安全紧急事件，为国家公共互联网、国家主要网络信息应用系统及关键部门提供计算机网络安全的监测、预警、应急、防范等安全服务和技术支持，及时收集、核实、汇总、发布有关互联网安全的权威性信息，组织国内计算机网络安全应急组织进行国际合作和交流。2001 年 10 月，信息产业部提出建立计算机应急响应体系，并且要求各互联网运营单位成立应急响应组织。自此我国建立起信息安全应急响应体系。

为落实国家网络与信息安全应急管理要求，国家有关部门开展了多项信息安全应急工作。2008 年 4 月，为满足奥运会期间北京城市信息安全各领域的安全需求，北京成立了全国首个城市信息安全应急响应与处置中心，确保及时发现、跟踪、分析和确认有重大危害的信息安全事件，对其进行及时响应，降低社会领域重要信息系统面临的风险和可能造成的损失。2009 年 9 月，工信部、证监会在北京联合组织开展了网络与信息安全应急演练。2009 年 12 月，上海市经信委组织了上海世博会信息安全应急专项演练，检验了上海世博会信息安全应急指挥机制、协调机制和操作流程，促进了世博会信息安全应急体系建设。

在应急响应体系的标准研制方面，我国先后发布了多项应急响应国家标准，其中《信息技术 安全技术 信息安全事件管理指南》（GB/Z 20985—2007）描述了信息安全事件的管理过程，提供了规划和制定信息安全事件管理策略和方案的指南；《信息安全事件分类分级指南》（GB/Z 20986—2007）规定了信息安全事件的分类分级规范，用于信息安全事件的防范与处置，为事前准备、事中应对、事后

处理提供一个基础指南；《信息系统灾难恢复指南》（GB/Z 20988—2007）规定了信息系统灾难恢复应遵循的基本要求；《信息安全技术 信息安全应急响应计划规范》（GB/T 24363—2009）规定了编制信息安全应急响应计划的前期准备，确立了信息安全应急响应计划文档的基本要素、内容要求和格式规范。

5．标准化工作

信息安全标准化工作以标准体系建设为基础，以确保国家信息安全为基本出发点，做好标准定制工作，在与国际标准相衔接的前提下，强化自主创新，促进产业发展。在编制研制方面，全国信息安全标准化技术委员会坚持以抓紧制定国家信息安全保障体系建设急需的、关键的标准为重点，积极开展标准制修订工作，已申报信息安全国家标准 204 项，其中 144 项已批准列入国家标准制修订计划。截至 2013 年年底，共组织申报信息安全国家标准 290 项，其中 249 项已批准列入国家标准制修订计划，正式发布国家标准 140 项。在发布的 140 项国家标准中，采用国际标准的有 35 项，参考国外先进标准制定的有 18 项，我国自主制定的标准有 87 项，自主制定标准比例达 62%。这些标准主要涉及信息安全技术与机制（42 项）、信息安全管理（27 项）、信息安全评估（66 项）及保密、密码和通信安全等（比例为 4%）领域[107]。

在电子政务信息安全标准体系建设方面，2010 年 2 月 1 日，国家标准《信息安全技术 基于互联网电子政务信息安全实施指南》（GB/Z 24294—2009）正式实施，该标准基于互联网电子政务信息安全总体架构，从安全技术、安全管理和安全自评估等方面提出了安全保障技术要求，并从需求分析、方案设计、系统实施与集成、系统试运行与完善、系统安全评估和正式运行等工程实施重要环节提出了信息安全工程实施方面的要求。

此外，我国还制定了其他通用的信息安全标准。《信息安全技术 信息安全风险管理指南》规定了信息安全风险管理的内容和过程，为信息系统生命周期不同阶段的信息安全风险管理提供指导；《信息技术 安全技术 信息安全管理实用规

[107] 百度文库．[EB/OL].http://wenku.baidu.com/link?url=Y9yqREajFsfzJl4UYhGwShQC1GW53by_CkRxrJ62DRatgVoIvaoeEoVfPq5ZAeMBJ0l4GtywOOOTgErTGNUJR2vXtHS9nRkR6gTdgaxDAOO.

则》给出了一个组织启动、实施、保持和改进信息安全管理的指南和一般原则；《信息安全技术 信息系统安全管理要求》规定了信息系统安全所需要的各个安全等级的管理要求，等等。这些标准对电子政务信息安全工作具有重要的指导意义。

3.2.4　电子政务网络和系统安全体系

我国在一些重要领域开展了电子政务基础设施建设，如电子政务网络建设、“金字工程”的启动、四大数据库的建设（人口、法人、地理信息和资源、宏观经济）、电子政务业务系统的建设、部委电子政务试点示范工程等，并在这些基础设施的安全保障方面做了大量工作。

1．政务外网安全保障

国家电子政务外网主要是为了满足国家各级政务部门社会管理、公共服务等面向社会服务的需要而建设的国家电子政务网络。国家电子政务外网是政务信息资源的汇聚点和集散中心，可以为政府实现网络资源的整合、信息资源共享、业务协同等创造一个良好的基础环境。根据中办发〔2002〕17 号提出的建设任务，中办发〔2006〕18 号文件《国家信息化领导小组关于推进国家电子政务网络建设的意见》提出了建设国家电子政务外网的目标，并要求通过建立统一的密码和密钥管理体系、网络信任体系和安全管理体系，分级、分层、分域保障电子政务网络信息安全。目前，电子政务外网工程经过近 10 年的规划、设计、验证、实施等过程，一期工程已于 2009 年年底通过竣工验收。在国家电子政务外网二期工程建设中，将围绕深化“放管服”改革、构建“互联网+政务服务”新业态等重大任务，以信用信息共享、投资项目审批监管、公共资源交易等国家重大工程建设及其应用和大数据分析为契机，依托政务外网二期工程建设提升网络安全和运维服务能力，推动政务外网向开放创新、集成利用、协同共享、安全高效发展[108]。

政务外网承载了一批中央的电子政务应用系统，其中，国务院应急平台外网业务在政务外网上实现了 24 个部委、35 个地方应急机构间的视频会议、图像及

[108] 资料来源：http://www.sic.gov.cn/News/79/6574.htm。

数据共享与交换业务；中纪委监察部“纠风系统”基于政务外网受理和办理群众举报、投诉、咨询和建议，向公众提供投诉和反馈服务；文化部的文化信息资源共享平台利用政务外网实现了与各省的高速互联和双向传输，每年更新数据达到10.5TB；“金安”工程利用政务外网构建了国家安全监管总局到 50 个省级节点的网络平台。

在政务外网信息安全保障方面，中办发〔2002〕17 号文件首先提出了要建设和整合统一的电子政务网络平台。从安全角度考虑，我国电子政务网络建设由政务内网和政务外网构成，两网之间物理隔离，政务外网与互联网之间逻辑隔离。

2008 年，国家发改委发布了多个文件，对电子政务工程建设的信息安全保障工作提出了明确要求和工作目标。2009 年，国家发改委和财政部联合印发了《关于加快推进国家电子政务外网建设工作的通知》（发改高技〔2009〕988 号），提出了促进国家政务外网信息资源共享和业务协同、加强安全保障和运维服务等工作要求，指出要“加强国家政务外网的信息安全保障工作”。2014 年 11 月 13 日，国家电子政务外网管理中心正式发布《国家电子政务外网信息安全标准体系框架》、《国家电子政务外网信息安全标准化工作规范》、《国家电子政务外网安全接入平台技术规范》、《国家电子政务外网安全监测体系技术规范与实施指南》、《国家电子政务外网安全管理系统功能技术要求与接口规范》、《国家电子政务外网跨网数据安全交换技术要求与实施指南》和《接入政务外网的局域网安全技术规范》7 项安全标准，为规范国家电子政务外网信息安全标准体系建设，指导各级政务外网开展安全接入、安全交换、安全监测，以及各级政务部门局域网安全连接政务外网等技术管理工作提供了依据[109]。

中央和地方政务外网的建设和运维单位，要切实落实网络安全保障责任制，明确国家政务外网信息安全主管领导和工作部门，建立健全安全管理制度。要按照国家政务外网统一规划，建立网络安全防护体系和统一的网络信任体系。要定期对中央和地方政务外网进行安全检查，对查出的安全隐患和问题及时进行整改，确保国家政务外网的安全可靠。

[109] 国家电子政务外网管理中心正式印发《国家电子政务外网信息安全标准体系框架》等七项安全标准[EB/OL].http://www.sic.gov.cn/News/306/4007.htm.

2．政务资源数据库安全保障

中办发〔2002〕17 号文件指出，要规划和开发重要政务信息资源，“启动人口基础信息库、法人单位基础信息库、自然资源和空间地理基础信息库、宏观经济数据库的建设”。目前，我国在部分数据库的建设方面取得了一定的成效，并在建设运维过程中注重统筹规划和信息安全保障。

人口和计划生育部门负责人口数据库的建设，目前已建立了育龄妇女信息、实行计划生育的老年夫妇信息、计划生育独生子女伤残死亡信息、人口和计划生育工作人员信息及人口和计划生育决策支持 5 个数据库[110]，建立了 21 项技术标准和业务规范，建立了信息安全体系和系统管理平台。

“法人单位基础信息库”是国家电子政务工程建设的重要任务，法人库项目建设由国家质检总局牵头，中央编办、民政部、国家税务总局、国家工商总局、国家质检总局、国家统计局等部门参加，共同建设以法人单位组织机构代码为统一标识，以编办、民政、工商、质检等部门对法人管理的注册登记、变更、注销等法人信息为依据的法人单位基础信息库，实现法人库与各部门的信息交换，实现法人单位基础信息采集的标准化和信息动态维护、反馈机制的制度化，为国家电子政务、社会和市场监管、法人信息公开打下信息化基础[111]。

国家自然资源和地理空间基础信息库的目标是依托已有信息化基础设施，按照统一标准规范，整合、改造项目参加单位现有的信息资源，通过建设基础性自然资源专题信息库、基础性地理空间专题信息库、自然资源与地理空间综合信息库和地理空间信息交换系统，形成自然资源和地理空间信息库数据主中心和 11 个数据分中心，以进一步增强国家对区域发展和资源环境进行宏观监管和动态监测、预测的能力，促进各部门自然资源和地理空间信息的共享，并为社会公众提供有关自然资源和地理空间的信息服务[112]。2014 年，在国家自然资源和地理空间基础信息库（以下简称信息库）各参建部门和单位的共同努力下，信息库项目建设

[110] 中国信息年鉴 2010[M]. 北京：中国信息年鉴期刊社，2010：135-136.

[111] 全国组织机构代码管理中心——法人库[EB/OL].http://www.nacao.org.cn/publish/main/7/index.html.

[112] 自然资源和地理空间基础信息库简介[EB/OL]. http://www.cstc.org.cn.

任务已全部完成，并顺利完成了初步验收工作，分别于 3 月 26 日、4 月 2 日和 4 月 22 日组织召开了财务、档案、工程与技术 4 个分项竣工验收会议。4 个分项竣工验收的顺利完成，为信息库项目后期的总体竣工验收和运行工作奠定了良好基础[113]。

宏观经济数据库是 2002 年列入中央电子政务一期重点建设项目的国家基础数据库之一，由国家统计局牵头承担建设工作。国家宏观经济数据库（一期）项目主要建设内容包括：① 制度规范建设。建立国家宏观经济指标体系和标准目录，将宏观库的业务纳入相关制度、法规框架之内，并遵循国家及电子政务相关技术标准。② 基础平台环境（含安全）建设。依托国家电子政务网络平台，建立宏观经济数据库共建单位之间互联互通、数据协同、安全可信、信息资源共享的基础平台环境[114]。目前，一期工程已基本完成了建设任务，初步实现了宏观经济管理部门间的互联互通和信息资源共享。在安全保障体系建设方面，依据信息内容和授权管理的原则，划分不同的安全域和信任域，制定相应的安全策略和安全措施，实施等级保护，构建系统信息安全保障体系[115]。

3．业务系统安全保障

从 2002 年颁布 17 号文件明确了“加快 12 个重要业务系统”的任务开始，我国政务信息资源基础设施建设历经数年发展，取得了实质性的进展。特别是以“十二金”为基础，拓展成为涉及国计民生的更多“金字工程”和重大项目，获得了良好的社会效益。“金字工程”取得了显著成绩，是电子政务建设的重要组成部分，各项工程在建设过程中非常注重信息安全保障工作。例如，“金财”工程于 2008 年完成了涉密网存储系统和内网备份系统建设工作，建立了完整的本地数据存储备份体系，实现了涉密网、内网、外网所运行的财政业务系统数据的集中存储和自动备份[116]；“金保”工程开展了全国统一的基于 PKI/CA 技术的人力资源

[113] 国家自然资源和地理空间基础信息库[EB/Ol]. http://www.gov.cn/xinwen/2014-06/06/content_2695243.htm.

[114] 中国经济的助跑器——宏观经济数据库[EB/OL]. http://www.thldl.org.cn/news/1009/49149.html.

[115] 中国信息年鉴 2010[M]．北京：中国信息年鉴期刊社，2010：200.

[116] 中国信息年鉴 2009[M]．北京：中国信息年鉴期刊社，2009：196.

社会保障网络安全信任体系建设，印发了《关于建设统一的人力资源社会保障网络安全信任体系的指导意见》，制定了相关的标准规范，开展了部本级容灾备份系统建设[117]；“金信”工程完成了工商总局信息系统安全等级保护定级工作，实行了内外网物理隔离，完成了工商总局“金信”工程一期安全系统项目建设[118]。

现代工业控制系统（ICS）包括过程控制、数据采集系统（SCADA），分布式控制系统（DCS），程序逻辑控制（PLC），以及其他控制系统等。工业控制系统是关键基础设施的基础，目前已应用于电力、水力、石化、医药、食品、汽车、航天等工业领域，成为国家关键基础设施的重要组成部分，关系到国家的战略安全[119]。《国家信息安全标准化“十一五”规划》特别将制定 ICS 的安全标准作为“十一五”期间信息安全标准化工作的重点。2010 年 10 月，工信部下发《关于加强工业控制系统信息安全管理的通知》（工信部协〔2011〕451 号），明确了重点加强核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热及其他与国计民生紧密相关领域的工业控制系统信息安全管理，落实安全管理要求，具体包括加强系统和网络防护、加强设备管理、加强应急管理、强化灾备措施、加强组织领导等。2010 年 1 月 21 日，工信部公布了《通信网络安全防护管理办法》，围绕通信网络安全防护管理工作，建立了 4 种主要制度：通信网络单位的分级保护制度；符合性评测制度；安全风险评估制度；通信网络安全防护检查制度。2011 年 10 月 25 日，工信部印发了《关于加强工业控制系统信息安全管理的通知》，提出要建立工业控制系统安全测评检查和漏洞发布制度。

3.2.5　信息安全技术和产业

为了鼓励和促进发展信息安全技术和产业，国家出台了一系列规划和政策措施。《2006—2020 年国家信息化发展战略》指出要“积极跟踪、研究和掌握国际

[117] 中国信息年鉴 2009[M]. 北京：中国信息年鉴期刊社，2009：205.
[118] 中国信息年鉴 2010[M]. 北京：中国信息年鉴期刊社，2010：192
[119] 石勇等. 工业控制系统（ICS）的安全研究[J]. 网络安全技术与应用，2008（4）.

信息安全领域的先进理论、前沿技术和发展动态，抓紧开展对信息技术产品漏洞、后门的发现研究，掌握核心安全技术，提高关键设备装备能力，促进我国信息安全技术和产业的自主发展”。《国务院关于加快培育和发展战略性新兴产业的决定》（国发〔2010〕32 号）表示，要“加快建设宽带、泛在、融合、安全的信息网络基础设施，推动新一代移动通信、下一代互联网核心设备和智能终端的研发及产业化，加快推进三网融合，促进物联网、云计算的研发和示范应用”。

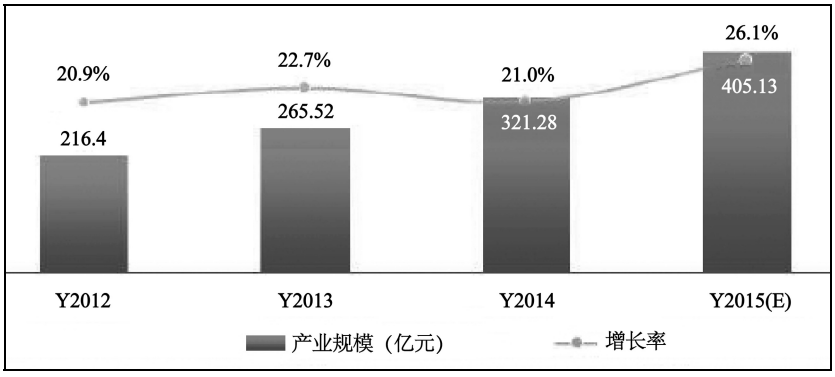
国家对信息安全技术研发和产业化的支持力度不断加大，信息安全产业保持平稳较快增长，信息安全服务业快速发展。国家自然科学基金、国家 863 计划和支撑计划、国家发改委信息安全专项继续加大对信息安全关键理论、技术研究和产业创新的支持力度，促进了技术创新和产业发展。2000 年，中国人民银行出台了国家第一个行业型的信息系统安全技术规范，证券、电信、电力、民航、铁路等行业也加大了信息安全投入，推动了信息安全产业的发展。2002 年，我国成立了中国信息产业商会信息安全产业分会，我国信息安全产业开始对国家基础设施信息化安全开展工作。目前，我国信息安全产业产品门类日益齐全，产业结构逐步调整，产业规模不断壮大。2015 年，我国信息安全产品市场规模达到 226.8 亿元，同比增长 18.5%，预计到 2017 年市场规模将接近 463 亿元[120]。根据中国信息安全等级保护网可知，我国的信息安全保护已成为包含定级备案、测评整改、监督管理等的较为完整的体系，相关测评机构和政策标准也较为完善，信息安全产品管理工作的规范化、制度化水平不断提高[121]。其中，本地数据备份与恢复、安全管理平台、身份鉴别、不可否认性鉴别、远程主机监测、IPS、小型防火墙等产品技术成熟、性能稳定；安全审计、物理隔离、网页恢复等产品在技术上有了较大改进和提升；防火墙等产品呈现出向更高性能发展的趋势，产品竞争力增强。此外，VPN、公钥基础设施（CA）、安全终端计算机系统、文件加密、不可否认性、完整性鉴别等产品应用日趋广泛，数量不断增多。

我国在关键信息技术领域突破发达国家技术垄断，取得了一定成绩。CNGI-CERNET2 和高性能计算技术在整体技术水平上进入世界领先行列，我国在

[120] CCID：2014—2015 年度中国信息安全产品市场研究年度报告[R].2015.

[121] 中国信息安全等级保护网[EB/OL].[2011-05-17].http://www.djbh.net/webdev/web/HomeWebAction.do?p=init.

下一代互联网关键技术上获得了突破性进展。世界第三代移动通信（3G）三大标准之一的 TD-SCDMA 标准，作为我国在通信标准领域的首次重大突破，对改变我国移动通信产业长期受制于人的状况、提高我国移动通信产业的国际地位具有十分重要的意义，其发展也为我国新一代移动通信标准与技术的演进奠定了基础。在 WiMAX 领域，产业规模快速增长，国内产业具有较强的竞争力，我国以华为、中兴为代表的中国通信制造企业加强了企业之间的合作，参与了 WiMAX 的标准制定和专利申请工作。虽然专利申请不多，但都深入 WiMAX 标准的核心领域，多项专利被纳入标准。我国在物联网等信息技术前沿领域均取得可喜成果。2010 年，我国推出了全球首颗拥有完全自主知识产权的二维码解码芯片，实现了硬件解码，使解码速度提高 10 倍以上，识读效率提高 30～50 倍，同时大大简化了原有解码系统所需的周边电路及其元器件，降低了成本和功耗，提高了可靠性。我国信息安全产品的自主创新工作取得了可喜的成绩，对 Hash 函数等信息安全基础理论的研究取得了重要突破；具有自主产权的安全芯片在防火墙、防病毒等领域得到应用；网络信息内容检测技术与组织体系得到了进一步发展。图 3-2 展示了 2012—2015 年我国信息安全市场增长情况。



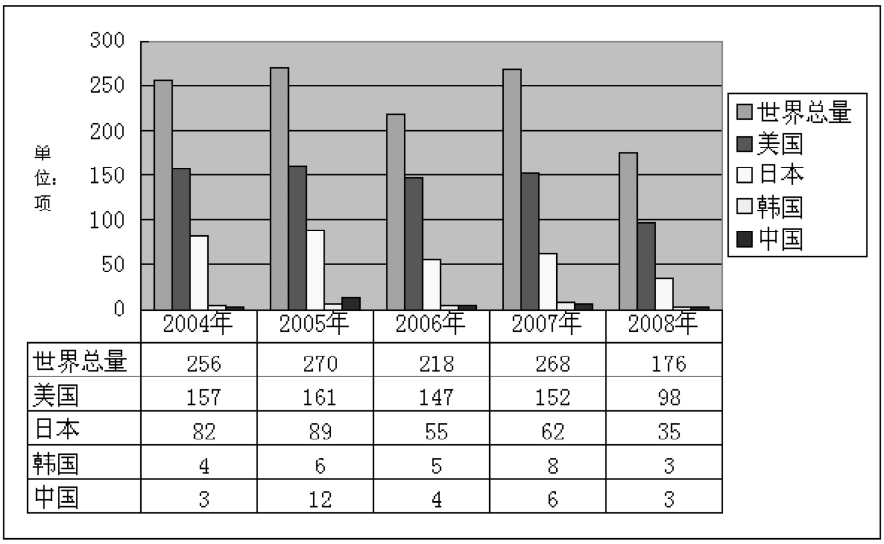
数据来源：赛迪顾问

图 3-2　2012—2015 年信息安全市场增长情况

但是，当前我国电子政务自主品牌产品严重不足的局面仍没得到根本改变。电子政务工程采购的软硬件产品中，自主品牌产品的采购金额还不到采购总额的 4 成；国产软硬件产品主要集中在中低端，高附加值的高端产品基本为国外产品；

核心的软硬件产品基本为国外垄断；国家电子政务工程建设对自主产业的拉动作用明显不足[122]。出现以上情况的原因主要表现在我国信息技术装备的核心技术研发能力较为薄弱、对重要信息技术的标准制定没有形成体系、以政府采购促进技术创新的政策措施仍需进一步完善等。具体表现在：

第一，我国芯片和极大规模集成电路设计等核心技术与国外相比还存在较大的差距（见图 3-3）。我国的芯片产业主要从事测试、封装等处于产业链低端的工作，核心技术较为落后，企业依附于跨国公司，产业缺乏主导权。2010 年我国有 65～75 条芯片制造线，我国在集成电路领域占世界市场份额的 5%～6%，成为世界集成电路芯片制造基地之一。但中国生产的芯片没有自主产权，这使得企业利润微乎其微，产业处于价值链低端。一方面，国内大量资金流失于购买国外专利的使用权，中国芯片产业链各环节真正从芯片中获得的利润非常少，整个芯片产业相当于在给别人打工，无形中在帮别人挣钱；另一方面，企业利润少，用于研发的经费就少，进一步制约了自主创新的进程。



	2004年	2005年	2006年	2007年	2008年
世界总量	256	270	218	268	176
美国	157	161	147	152	98
日本	82	89	55	62	35
韩国	4	6	5	8	3
中国	3	12	4	6	3

数据来源：世界专利索引数据库

图 3-3　2004—2008 年极大规模集成电路关键技术领域专利拥有量

[122] 资料来源[EB/OL]：http://gjss.ndrc.gov.cn/gzdt/t20080422_205722.htm。

第二，标准和知识产权越来越成为跨国公司垄断技术和产业的手段，因此，实施技术标准和知识产权保护已经成为保障国家信息安全的重要战略。例如，“文档”是电子政务应用中的普遍性技术，而文档标准实际上与信息安全密切相关，掌握文档标准及关键技术的实体，可以通过平台和文档升级、反馈漏洞等理由来获取相关计算机的信息。再如，在极大规模集成电路关键技术方面，美国是拥有专利最多的国家，占专利总数的 63%；我国的专利数量仅占 2.1%，而核心技术如光刻、设计技术等尚未实现。

第三，在政策环境方面，我国政府采购促进自主创新的相关法律法规还不够完善，政府采购对自主创新的促进作用还远没有充分发挥出来。我国政府采购的研究起步较晚，对政府采购促进自主创新的作用还认识不足。过去我国对自主创新的激励主要通过财政、税收政策，而从对自主创新产品的采购方面进行支持，是最近几年人们意识到政府采购从市场需求的角度出发对一个国家的自主创新有着相当的促进作用后才提出来的。而西方发达国家早已将政府采购作为政府调整产业结构、促进自主创新的重要手段之一，理论和实践已经较为成熟。

3.2.6　人才培养与安全意识

近年来，我国国内高校信息安全专业建设、学位点建设等工作开展迅速。2005 年，教育部发布《关于进一步加强信息安全学科、专业建设和人才培养工作的意见》，指出要加快信息安全学科、专业建设和信息安全人才的培养。2007 年，教育部发布《教育部关于成立教育部高等学校信息安全类专业教学指导委员会的通知》（教高函〔2007〕1 号），成立了教育部高等学校信息安全类专业教学指导委员会，聘请专家、学者开展高等学校信息安全类本科专业教学的研究、咨询、指导、评估、服务等工作。2001 年，我国开始在高校中设置信息安全本科专业，形成了包括本科、硕士、博士、博士后的完整教育体系。目前，全国约有 70 余所高校设立了 80 个信息安全类本科专业，25 所高校和研究所设立了信息安全二级学科博士点，有 15 所高校获教育部批准建设信息安全特色专业，为我国信息安全产业的迅速发展培养了一批有知识、有能力、懂技术的高素质信息安全专业人才和管理型人才。

国家主管部门加大了对信息安全的宣贯培训力度。工业和信息化部每年举办信息安全培训班。2010 年，工业和信息化部举办了 2010 年中央国家机关信息安全培训班，面向来自国务院部委及直属机构共 69 个单位的 79 名信息安全处长及相关技术、管理人员，重点培训信息安全最新形势、技术发展趋势、信息安全管理、信息安全检查、信息安全最新实践等方面的内容。2010 年 10 月，工业和信息化部举办了 2010 年地方领导干部信息安全专题研究班，面向来自全国各省（自治区、直辖市）、新疆生产建设兵团工业和信息化主管部门分管信息安全工作的厅局级领导及部分城市分管信息安全工作的副市长（副专员）。2010 年 4 月，为贯彻落实《政府信息系统安全检查办法》等文件精神，工业和信息化部信息安全协调司举办了 2010 年地方政府信息系统安全检查专业机构技术培训，面向来自 24 个省（区、市）、3 个副省级城市承担政府信息系统安全检查任务的专业机构的工作人员。

3.3 对我国电子政务信息资源共享安全保障机制建设的启示

3.3.1 战略统筹需要加强

战略统筹是保障电子政务信息资源共享建设持续、有效的重要基础。世界发达国家和地区普遍重视电子政务信息资源共享建设的战略统筹工作，各国相继发布了多项国家级战略计划用于指导电子政务信息资源共享建设。在规划过程中，注重电子政务建设的系统性，同时将公民满意度、绩效评估等作为一项重要内容，不断改进电子政务建设。我国在电子政务信息资源共享的战略统筹方面也做出了一些有益的探索，在实际建设过程中，主要表现为一些省、市电子政务信息资源共享战略规划的制定。由于我国各地经济环境的差异性、电子政务建设起步情况不同及建设水平差异等因素的影响，各地战略规划的侧重点有所不同，致使战略规划系统性不强的问题较为突出。此外，对于电子政务信息资源共享建设的后期

评估还较为缺乏，评估方法、评估机制等亟待建立和完善。因此，我国电子政务信息资源共享建设在战略规划中应注重系统性，加强统筹、统一规划，并将后期评估逐步纳入电子政务信息资源共享建设之中。

3.3.2　领导体制和管理机制急需健全

领导体制和管理机制的健全是电子政务信息资源共享建设持续、有效的重要保障。世界发达国家和地区普遍重视电子政务建设的领导体制和管理机制建设，根据本国国情形成了各具特色的领导体制；重视管理机构的设置、管理和协调，强化对电子政务信息资源共享及信息安全工作的领导。我国在领导机制建设方面存在各自为政、职责不明确的现象，在管理机制和工作机制上缺乏宏观战略指导和微观策略实施的有效配合。以“金字工程”为例，纵向应用系统建设多由相应部门自行安排，有些跨部门业务系统则被牵头部门设计成部门内系统，由于缺乏统一指导和协调，导致各部门自建、自用、自成体系，网络、平台、标准各异，部门间信息资源共享和业务协同遭遇技术、管理等多方面的阻力。在管理机制方面，一是缺乏信息资源共享的申请和登记制度。有些部门面对信息资源共享的实际工作无从下手，信息资源共享经常陷入难以实施的被动局面。我们调研的 95 家单位中，80%以上的工作人员不清楚所共享信息的来源、去向和用途。二是缺乏激励机制。由于部门职能分工导致大量政务信息资源掌握在少数信息资源共享的“强势部门”手中，这些部门出于维护本部门利益和权威考虑，在信息资源共享中持消极态度，阻碍其他部门获取履行职能所需的信息资源，目前这一僵局尚缺乏有效的激励机制来打破。三是缺乏绩效考核机制。由于缺乏绩效考核机制的制约，使得信息提供方和需求方在政务信息资源共享具体实施中无法平衡其成本和收益，缺乏共享的积极性和主动性，阻碍了各部门做出有益于推动信息资源共享发挥效益的良性决策。此外，由于信息资源共享要从实施层面加以推动，对信息资源共享部门和实际工作者的绩效考核十分必要。因此，我国急需健全电子政务信息资源共享建设工作的领导体制和管理机制，管理机制方面尚需健全管理协调和规划落实的部署工作和相关流程、规定及责任制度。

3.3.3 法律法规体系应加速推进

法律法规体系的建立健全是电子政务信息资源共享建设持续、有效的重要保证。世界发达国家和地区普遍重视建立健全法律法规体系，制定和颁布了一系列法律法规和标准用于保障电子政务建设及电子政务信息资源共享安全。在我国电子政务的建设过程中，相继颁布和制定了相关的法律法规、标准，但现行涉及电子政务信息资源共享的立法大多属于部门规章或地方法规，法律层级较低，效力有限，缺乏国家统一指导协调电子政务信息资源共享的法律。如果不明确共享活动中各方主体的权力和责任，难免会让一些部门在信息资源共享工作中有诸多顾忌。此外，保障电子政务信息资源共享安全的《信息安全法》、《个人信息保护法》等相关法律的缺失，加大了政务信息资源共享的阻力。在落实已有法规的过程中，也存在着实施力度不够、宣贯程度不高等问题。因此，我国需要不断完善相关法律法规，制定相关标准，同时注重各项法规和标准的贯彻实施工作。

3.3.4 信息技术应用自主可控水平有待提高

世界发达国家和地区非常注重对信息通信关键技术的研发，加之我国信息安全技术产业竞争力普遍较弱，使得我国政府关键信息系统的核心软硬件、系统集成、关键设备和安全服务严重依赖国外厂商，重要信息系统的潜在安全隐患突出。我国电子政务系统中微软、IBM、HP、思科、甲骨文等国外软硬件仍占主流，电子政务工程采购的软硬件产品中，自主品牌产品采购金额还不到采购总额的 4 成。对于我国信息安全产业来说，由于缺乏明确有效的投融资政策和政府采购政策，国内信息安全企业普遍面临投融资难、市场推广难的困境。信息安全产品市场缺乏有效合理监管，价格恶性竞争和侵犯知识产权问题严重影响了企业盈利能力。信息安全服务缺乏有效规范，信息安全服务企业利润普遍较低。这些都是我国信息技术应用能力不高的原因。

3.3.5　信息安全保障能力有待提高

信息安全保障能力是电子政务信息资源建设成功与否的关键。世界发达国家和地区纷纷从信息安全关键技术研发、科技政策制定、信息安全人才队伍建设等方面提高信息安全的保障能力。对于我国来说，信息安全保障能力主要体现在安全防护能力、隐患发现能力、应急处置能力、信息对抗能力等方面。我国在电子政务信息资源共享建设过程中重视信息安全问题，但由于目前缺乏统筹性的信息安全保障战略，加上我国在信息安全关键技术、软硬件核心技术等方面与国际先进水平之间存在较大差距，使得我国信息安全整体保障能力无法满足电子政务信息资源共享安全保障的需求。另外，随着云计算、物联网等新技术在电子政务领域的广泛渗透，以及移动政务的快速发展，如果这些新技术的安全防范措施未得到及时跟进，则会给政务系统带来新的安全隐患。由于政务信息资源的重要性，我国急需加强信息安全保障的自主可控，加大国产软硬件的推广应用力度，制定积极的科技发展政策，不断强化我国的信息安全保障能力，为电子政务信息资源共享建设保驾护航。

第 4 章
电子政务信息资源共享的影响因素及安全风险分析

随着电子政务建设的深入推进，我国电子政务信息资源总量不断增加、质量不断提高，政府信息资源开发及共享环境得到逐步改善。但是从近年来的研究看，电子政务信息资源共享仍面临着诸多困境，如机构缺乏信息资源共享意识、跨部门信息资源共享程度低、行政管理体制机制的制约、信息资源共享成本与利益分配问题、信息技术和信息安全问题等，这些都严重影响了电子政务信息资源共享工作的顺利开展。本章以对跨部门信息资源共享中收益与风险的感知为立足点，对电子政务信息资源共享中的障碍、安全风险及管理机制等内容进行实证分析，探讨了影响电子政务信息资源共享的主要因素及其影响方式和程度。

4.1 电子政务信息资源共享的影响因素

通过对历史文献的梳理（见表 4-1）[123]，我们归纳出 11 项影响电子政务信息资源共享的因素，主要包括法规标准、信息素质、共享成本、领导力、社会网络、完整性、保密性、便利性、协同性、过程信任度和机构信任度，而电子政务中信息资源共享绩效可以用信息资源共享过程中感知到的收益和风险进行衡量[124]。基于这些认识，本章开发了影响电子政务信息资源共享过程中感知收益和感知风险的影响因素指标，并进行了调研分析。

表 4-1 变量及测量工具

变　量	题　项	参考文献
环境因素		
法律-政策层面	3	（Dawes，1996）
高层管理机构权威	1	（Grover，1993）
部门间关系		
部门间信任	6	（Zaheer，McEvily，& Perrone，1998）
社会网络关系	5	（Dawes，1996）
组织兼容性（标准）	5	（Dawes，1996）
部门内准备		
领导支持	2	（Dawes，1996）
运营成本	3	（Dawes，1996）
处理安全	3	（Dawes，1996）
IT 技术	1	自编
流程安全	4	（Landsbergen & Wolken，2001）
共享效果		
感知收益	5	（Gil-Garcia et al.，2007；Gil-Garcı-A & Pardo，2005）
感知风险	3	（Gil-Garcia et al.，2007；Gil-Garcı-A & Pardo，2005）

[123] 见 1.2.2 节。

[124] Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. Collaborative e-Government: Impediments and benefits of information-sharing projects in the public sector[J]. European Journal of Information Systems, 2007, 16(2):121-133.

续表

变　量	题　项	参考文献
安全保障		
保密性	3	自编，（Lambrinoudakis，2003）
完整性	1	自编，（Lambrinoudakis，2003）
便利性	2	自编，（Lambrinoudakis，2003）
纵强横弱	2	自编

本次调研的数据来源包括各省信息中心、各省信息化管理部门及信息化研究机构。调研向三种机构发放问卷的比例分别为 80%、15%、5%，共发放问卷 120 份，回收 95 份有效问卷，回收率为 79.2%。

4.1.1　自变量探索性因子分析

首先使用自变量的 11 个指标进行探索性因子分析。根据对相关文献和理论的分析，这些指标中应包含信息资源共享环境、共享的安全性和便利性、共享过程、机构的信任度 4 个因子。因此，提取因子的个数最好为 4 个，提取方法采用主成分分析法（Principal Component Analysis），并对因子进行方差最大化（Varimax）旋转。

如表 4-2 所示，测量题项之间相关性的 KMO 样本测度值为 0.707，巴特莱特（Bartlett）球形检验的近似卡方值为 282.903，统计量的显著性概率是 0.000，小于 0.01，适合进行因子分析。

表 4-2　自变量因子分析的 KMO 样本测度和 Bartlett 球形检验

KMO 样本测度	0.707	
Bartlett 球形检验	近似卡方值	282.903
	自由度	55
	p	0.000

从表 4-2 所示的结果来看，设计的电子政务信息资源共享 11 个指标可以被 4 个隐含的公因素所解释，各指标分别归属于对应载荷最大的因子，因子在各指标

上的载荷都大于 0.5，说明调查问卷在自变量各指标中具有足够的结构效度，即问卷足以准确测度影响电子政务信息资源共享的各因素的内容。测量信度用克朗巴哈系数评定，从表 4-3 中可以看出，4 个因子的克朗巴哈系数分别为 0.641、0.823、0.640 和 0.752，测量的内部一致性可以接受。4 个因子共解释了原有信息的 66.25%。

表 4-3　电子政务信息资源共享自变量指标因子分析结果

指　　标	因子 1	因子 2	因子 3	因子 4
法规标准	0.702			
信息素质	0.701			
共享成本	0.573		–0.509	–0.466
组织领导	0.550		0.458	
社会网络	0.526			
完整性		0.908		
保密性		0.888		
便利性			0.763	
协同性			0.657	
过程信任度				0.847
机构信任度				0.581
内部一致性系数	0.641	0.823	0.640	0.752
方差解释量	66.25%			

注：表 4-3 中只给予了 0.4 以上的因子载荷。

根据因子所对应的各指标含义，对 4 个因子（F1、F2、F3、F4）进行解释和命名如下。

F1：共享环境因素

第一个因子 F1 主要解释了电子政务信息资源共享的相关法规标准、实施人员的信息素质、领导力、社会网络及成本控制方面的内容，它反映了电子政务信息资源共享中的法律环境、人员配备、社会和经济环境等，是电子政务信息资源共

享的制度和环境层面，因此，称其为共享机制因素。由表 4-4 可知，在共享环境因素方面，虽然表现不尽如人意（3.198），但近年来，相关管理部门对电子政务信息资源共享的法律法规、相关人员培训、经济投入及领导重视程度等方面都有了很大的进步。

F2：共享安全因素

第二个因子 F2 主要是电子政务信息资源共享过程中的保密性和完整性。信息的保密性和完整性是信息资源共享安全性的主要方面，所以，F2 为共享安全性因素。它主要包括安全技术、安全管理和安全制度。安全因素仍然是电子政务信息资源共享中的主要障碍之一，在实施电子政务信息资源共享过程中，安全因素的表现仍然远不能让人满意（3.068），而且具有很大的不稳定性和难以控制性（标准差为 0.745）。因此，继续提高资源共享的安全技术、管理水平和完善安全保障制度仍然是今后电子政务实践的重要任务。

F3：共享便利程度

F3 主要表现为电子政务信息资源共享过程中部门之间的协同性和信息资源共享的便利性，这两方面共同保证了各部门可以顺畅地使用共享信息。因此，我们称 F3 为共享便利程度。我国目前的电子政务实践，信息资源共享的程度依然较低，共享范围还比较窄，并没有在普遍意义上实现共享，但可以看出在业已实施信息资源共享的部门中，共享的便利程度是受到一定认可的（3.609），这说明电子政务信息资源共享真正为部门间的信息交流带来了便利。

F4：共享信任度

F4 主要包含电子政务信息资源共享过程信任度和机构信任度，这一因素解释了各方在信息资源共享过程中的相互信任程度，因而叫作共享信任度因素。信任是以往的研究关注较少的一个方面，但却对信息资源共享有至关重要的影响。我国目前正处于电子政务信息资源共享的初始阶段，各部门对自身信息对外共享都具有一定的顾虑，对部门外的组织和个人可能会产生不信任因素，这严重影响了信息资源共享的主动性。表 4-4 显示，在电子政务信息资源共享过程中，信任因

素仍然是最主要的障碍（2.982）。部门间的信任很难在短期内通过技术手段和经济投入来获得，只有加强机制建设，明确各方的权责界限，才能逐渐消除信任方面的障碍。

表 4-4　电子政务信息资源共享自变量因子的描述性统计

因　子	题项数	均　值	标准差
F1（共享环境因素）	17	3.198	0.506
F2（共享安全因素）	4	3.068	0.745
F3（共享便利程度）	7	3.609	0.623
F4（共享信任度）	8	2.982	0.579

4.1.2　共享绩效变量的因子分析

由表 4-5 可以得到，KMO 值为 0.768，近似卡方值为 339.848，巴特莱特统计值的显著性概率是 0.000，小于 0.01，非常适合进行因子分析。因子分析的结果如表 4-6 所示，电子政务信息资源共享的 8 个绩效指标已经被分为两类，因子在各指标上的载荷都大于 0.7，且两个因子共同解释了原有信息的近 68%。

两个因子的克朗巴哈系数分别为 0.891 和 0.706，都比较理想，说明因变量测量量表的内部一致性很高。测量效度从以下几个方面评断：第一，由于所有的测量题项都来自成熟的研究，因此测量的表面效度和内容效度能够保证；第二，在所有题项中，没有一个题项在不同因子上的负载同时大于 0.5，说明测量具有较好的区分效度；第三，表 4-6 显示，两个因子的载荷均大于 0.7，高于参考值 0.5，这说明测量具有较好的聚合效度。综合以上分析可以判定，政务信息资源共享绩效的测量具有很好的信度和效度。

表 4-5　因变量因子分析的 KMO 样本测度和 Bartlett 球形检验

KMO 样本测度	0.768	
Bartlett 球形检验	近似卡方值	339.848
	自由度	28
	p	0.000

表 4-6　共享绩效指标的因子分析结果

	因　子	
	F5	F6
感知收益 3	0.875	
感知收益 2	0.872	
感知收益 4	0.823	
感知收益 5	0.819	
感知收益 1	0.773	
感知风险 2		0.853
感知风险 3		0.783
感知风险 1		0.732
方差解释量	67.75%	

根据因子所对应的各指标含义，对两个因子进行解释和命名如下。

F5：感知收益

感知收益是相关部门在实施电子政务信息资源共享后所感受到的有利方面，如成本节约、提高工作效率、提高公共形象等。

F6：感知风险

感知风险是与共享收益相对的，它是相关部门在实施信息资源共享后感受到的不利方面，如外界不合理的干涉、公众的误解和误用等。如表 4-7 所示，实施电子政务信息资源共享的感知收益远大于感知风险。

表 4-7　共享绩效因子的描述性统计

因　子	题 项 数	均　值	标 准 差
F5（感知收益）	5	3.830	0.659
F6（感知风险）	3	2.691	0.617

4.2　模型及假设的提出

电子政务信息资源共享的安全性、便利性及共享过程和机构的信任度，反映

了电子政务信息资源共享的安全态势，相关人员和部门的感知风险与感知收益则是电子政务信息资源共享绩效的表现。基于以上分析，我们建立如下概念模型（见图 4-1）来研究共享机制和安全因素对电子政务信息资源共享的影响，旨在探索规避电子政务信息资源共享风险、提高安全保障能力的对策和机制。

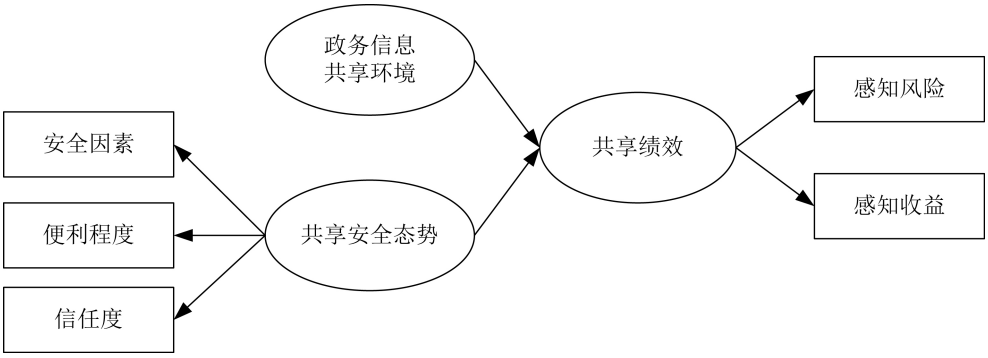


图 4-1　共享环境、安全态势与电子政务信息资源共享的概念模型

根据以上分析，提出如下研究假设。

H1：政务信息资源共享环境因素对感知收益有显著的正向影响。

H2：政务信息资源共享安全因素对感知收益有显著的正向影响。

H3：政务信息资源共享便利程度对感知收益有显著的正向影响。

H4：政务信息资源共享信任度对感知收益有显著的正向影响。

H5：政务信息资源共享环境因素对感知风险有显著的负向影响。

H6：政务信息资源共享安全因素对感知风险有显著的负向影响。

H7：政务信息资源共享便利程度对感知风险有显著的负向影响。

H8：政务信息资源共享信任度对感知风险有显著的负向影响。

4.3　假设检验

4.3.1　相关性分析

在进行回归分析之前，首先对被解释变量和解释变量之间的相关性进行分析。各变量之间的 Pearson 相关系数如表 4-8 所示。从表 4-8 中可以看出，感知收益和所有 4 个因素都在 0.05 以上的水平上有显著的相关关系，而感知风险只与共享信任度在 0.05 的显著性水平上相关，而与其他 3 个因素均不显著相关，初步验证了假设 1～4 和假设 8。同时说明信任在电子政务信息资源共享方面的作用，信任显著地影响感知风险，信任度的不足已经成为急需解决的首要问题。

表 4-8　被解释变量和解释变量之间的相关性分析

	F1	F2	F3	F4	F5
F1（共享环境因素）	1				
F2（共享安全因素）	0.330***				
F3（共享便利性）	0.437***	0.418***			
F4（共享信任度）	0.285**	0.211*	0.19		
F5（感知收益）	0.287**	0.377***	0.546***	0.247*	
F6（感知风险）	0.192	0.095	0.051	–0.255**	–0.16

注：* p<0.05，** p<0.01，双尾检验。

4.3.2　回归分析

下面分别以共享收益和共享风险为被解释变量进行回归分析，结果如表 4-9 所示。

表 4-9 显示，两个回归方程的 F 检验都是显著的，每个模型都有一些回归系数显著异于零，模型的 Durbin-Watson 值均在较好的范围内，这说明各个模型的

总体回归效果较好，引入的解释变量也是有效的。

表 4-9　电子政务信息资源共享表现各维度对感知收益和感知风险的回归结果

变量	感知收益	感知风险
常数项	1.225(.450)**	2.622(.478)***
共享环境因素	0.000(.129)	0.340(.137)
共享安全因素	0.142(.085)*	0.078(.091)
共享便利程度	0.482(.106)***	–0.043(.113)
共享信任度	0.145(.103)	–0.369(.109)***
R^2	0.340***	0.148**
Adjusted R^2	0.311***	0.110**
R^2 变化	0.340***	0.148**
F（变化）值	11.605	3.918
Sig. F（变化）值	0.000	0.006
Durbin-Watson	2.263	1.733

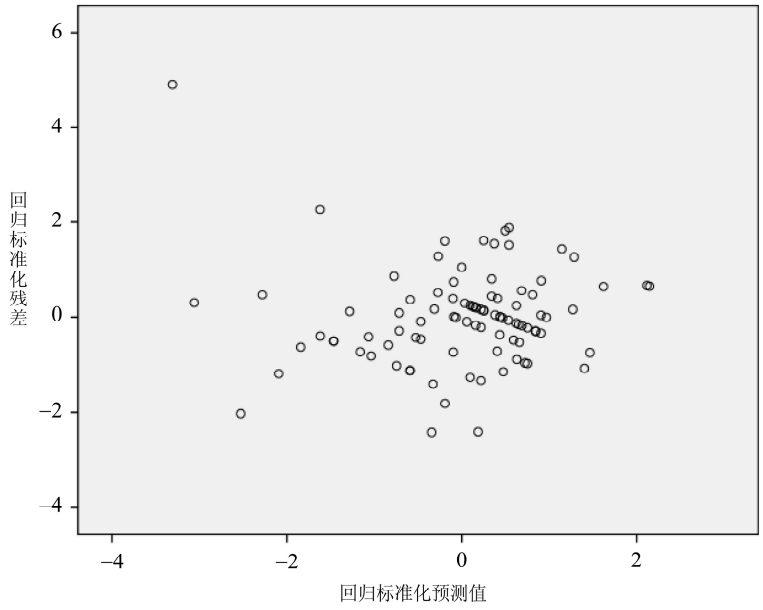
注：a．每个解释变量前第一个参数是非标准回归系数，第二个参数（括号内的参数）是标准差；

b．*p<0.05，**p<0.01，***p<0.001，双尾检验。N=95。回归方法为强制回归法。

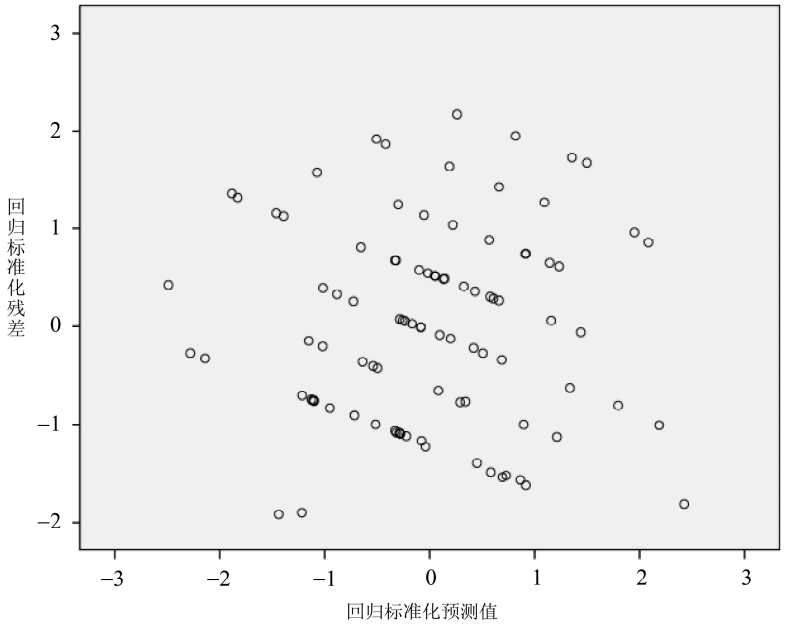
模型采用的主成分回归方法可以解决多自变量回归的多重共线性问题，接下来要检验两个回归方程的异方差问题。以被解释变量的标准化预测值为横坐标、以其回归标准化残差为纵坐标绘制散点图，结果如图 4-2 所示。从图 4-2 中可以看出，绝大部分观测变量都随机落在(–2,2)范围内，预测值和标准化残差没有明显的关系，说明两个回归模型满足方差齐性假设，不存在异方差问题。

最后检验模型的序列相关问题。由表 4-9 可以看出，模型的 Durbin-Watson 值分别为 2.263 和 1.733，非常接近 2，这说明相邻编号的样本值之间不存在序列相关问题。

比较模型 1 与各变量之间的相关系数，可以看出，与感知收益有关的共享环境因素和共享信任度在模型 1 中的 β 值并不显著，但是共享环境因素和共享信任度与感知收益之间确实有相关关系，这说明在模型 1 中，共享环境因素可能影响其他变量，从而影响感知收益。



（a）感知收益



（b）感知风险

图 4-2　被解释变量的回归标准化预测值与标准化残差散点图

共享环境因素是宏观层面的制度及其他因素，可能对共享安全因素、共享便利因素或共享信任度有影响，从而对感知收益有预测作用。因此，我们假设共享安全因素、共享便利因素、共享信任度中介了共享环境因素对感知收益的影响，对共享安全因素、共享便利因素和共享信任度的中介效应进行检验，结果如表 4-10～表 4-13 所示。

表 4-10　共享安全因素在共享环境因素与感知收益间的中介效应

变　　量	感知收益	感知收益
自变量		
共享环境因素	0.287***	0.061
中介变量		
共享安全因素		0.52***
F	8.378	19.825
R^2	0.083	0.301
ΔR^2		0.219

表 4-11　共享便利因素在共享环境因素与感知收益间的中介效应

变　　量	感知收益	感知收益
自变量		
共享环境因素	0.287***	0.183
中介变量		
共享便利因素		0.317***
F	8.378	9.553
R^2	0.083	0.172
ΔR^2		0.089

表 4-12　共享安全因素在共享信任度与感知收益间的中介效应

变　　量	感知收益	感知收益
自变量		
共享信任度	0.247***	0.176
中介变量		

续表

变　量	感知收益	感知收益
共享安全因素		0.340***
F	6.065	9.525
R^2	0.061	0.172
ΔR^2		0.111

表 4-13　共享便利因素在共享信任度与感知收益间的中介效应

变　量	感知收益	感知收益
自变量		
共享信任度	0.247***	0.149
中介变量		
共享便利因素		0.518***
F	6.065	21.606
R^2	0.061	0.319
ΔR^2		0.258

比较两个模型可以发现，影响电子政务信息资源共享实施部门的感知收益和感知风险的因素存在着较大的差异。共享的安全性和便利性显著地正向影响着感知收益，共享便利性的影响程度还较大（0.482），H2 和 H3 成立。在表 4-9 中，H1 和 H4 似乎并没有得到支持，但是考虑到共享环境因素和共享信任度在共享过程中的重要性，以及表 4-8 中较强的相关系数，因此，本研究认为共享环境因素和共享信任度可能并非直接对感知收益有影响，而是通过其他影响因素（例如安全因素和便利因素）对感知收益产生影响。接下来分析共享安全因素和共享便利因素的中介效应。

从表 4-4～表 4-13 中可以看出，共享环境因素通过影响共享安全因素和共享便利因素对感知收益产生正向影响作用，共享信任度也通过共享安全因素和共享便利因素对感知收益产生正向的影响作用，H1 和 H4 得以验证。H1 得以支持，说明相关的法律标准、人员配置和社会网络设计等营造了一个实施电子政务信息资源共享的政策环境，并发挥着重要作用。

从结果可知，部门对电子政务信息资源共享的收益感知直接来自信息资源共享的安全性和便利性方面。安全性和便利性是进行信息资源共享时要考虑的重要因素，共享信任度虽不能对收益产生直接的有益影响，但却能通过影响共享安全性和便利性间接影响信息资源共享的绩效。同时 H8 得以验证，说明信任的缺失会产生显著的较大的感知风险，因而信任是重要的保障性因素，它是共享安全和便利性等效用性因素发挥作用的前提条件。组织间的信任构成了实施电子政务信息资源共享的极为重要的软环境，只有在组织间充分信任的基础上，共享的机制设计（法规标准、人员配备、社会网络等）、共享资源安全性、便利性等的措施才会较好地发挥作用。

H6 没有被支持是一个比较意外的结论。在大多数研究中，电子政务信息资源共享的安全性是风险的主要来源，也构成了信息资源共享的一个重要障碍，但这里的结论提醒我们，组织间的信任度严重制约着电子政务信息资源共享，信任的缺乏导致了组织间感知的扭曲，成为瓶颈性的风险因素。在心理学研究中，感知风险是被调查者的主观判断，和实际风险还有一定的距离，所以它更容易受同是主观因素的信任度的影响，而且组织间的信任相对于业务性更强的共享安全性更容易被组织内人员所感知。H7 没有被支持，也缘于在我们的研究中信息资源共享的便利性主要与收益相关，并不是风险的主要来源。

综上所述，回归方程不存在异方差和序列相关问题，而多重共线性也由主成分回归避免，因而模型所支持的结论具有一定的合理性，可以作为政策分析的依据。

4.4 电子政务信息资源共享的影响因素分析

前面利用因子分析的方法对多种影响因素提取公因子，最终找到 4 个高阶的影响因素，分别是共享环境因素、共享安全因素、共享便利程度和共享信任度。通过研究这 4 个高阶的影响因素对信息资源共享过程中的感知收益和感知风险的影响，得出如下结论。

4.4.1　安全风险贯穿于电子政务信息资源共享的整个周期

电子政务信息资源共享的安全风险无处不在，存在于信息存储、传输、交换、处理的各个阶段。信息在存储过程中面临着被敌手篡改的风险，在传输过程中面临着被截获的风险，在交换过程中面临着被泄露的风险，在处理过程中则面临着被误操作的风险。

拥有重要信息系统的部门，通常都会担心信息资源共享会增加系统的安全隐患，如病毒侵害、黑客攻击、程序故障等，这些安全风险成为开展电子政务信息资源共享工作的一大障碍。因此，信息安全保障能力是电子政务信息资源建设成功与否的关键。由于政务信息资源的重要性，我国急需加强信息安全保障的自主可控，加大国产软硬件的推广应用力度，制定积极的科技发展政策，不断强化我国的信息安全保障能力，以此来积极应对电子政务信息资源建设面临的安全风险。

4.4.2　安全因素和便利程度是电子政务信息资源共享考虑的首要因素

电子政务信息资源共享一方面能够提高政府的行政执行力、政策实施力、政策实施的准确性和有效性，不断改善政府的管理和服务，提高政府办事效率、方便公众；但另一方面，大量的政务信息资源事关国家政治安全、经济安全、国防安全和社会稳定，如果这些信息被泄露或被不正当利用，则会对国家安全、公民隐私、单位财产构成严重威胁，后果不堪设想。

安全因素成为电子政务信息资源共享考虑的首要因素。这些安全因素不仅包括信息在存储、传输、交换和处理过程中的保密性、完整性、真实性、可用性和抗抵赖性，同时需要考虑的安全因素还应包括系统的预警、保护、检测、响应、恢复和反击等能力。调研发现，多数部门对信息资源共享可能带来的安全风险有所顾忌，不少单位以害怕引发安全问题为由拒绝为其他单位提供共享信息。

信息资源共享的便利程度主要与收益相关，并不是风险的主要来源。电子政务信息资源是政府在履行职能过程中产生或使用的信息，为政务公开、业务协同、辅助决策、公共服务等提供信息支持，给信息资源共享机构带来了经济和社会效益：一方面，信息资源共享能够降低信息利用成本，提高信息的效率和作用；另一方面，共享能够克服由于政府职能部门之间分工不同造成的信息不完全和非对称性对电子政务工作带来的困难，提高政府的工作效率。

电子政务信息资源共享建设需要同时考虑安全和便利程度的因素，因此，在我国电子政务信息资源共享建设实践中，可以通过加强战略统筹来合理、有效地解决共享中的安全问题，以提高政府服务的效能。

4.4.3 组织间的信任保障是实施电子政务信息资源共享的基础

组织间的信任是实施电子政务信息资源共享极为重要的软环境，如果缺失，将严重制约着电子政务信息资源共享。信任的缺乏导致了组织间感知的扭曲，成为瓶颈性的风险因素。信任是群体合作的基础，也是经济、社会协调发展的前提条件。民无信不立，信任是社会活动的基本前提。同样，在政务活动中，政府机构之间、政府与公众之间、政府与企业之间信任关系的建立，是电子政务得以推广应用的关键，是实现信息资源共享和跨部门、跨地区协同办公的基础。

从目前来看，电子政务信任机制尚未建立，主要表现在以下几个方面。

1．对网络的不信任

由于网络环境中的身份难识别、责任难确定、权限难控制等因素，给网络信任机制建设带来了很大的困难。拥有重要信息系统的部门，一般都担心共享会增加系统的不安全性，如病毒侵害、黑客攻击、程序故障等，成为政务活动中各利益方开展工作的一个障碍。

2．对信息的不信任

西蒙曾说“信息是管理的基础”，信息的准确性是做好电子政务工作的关键。

在过去，尽管一些单位积累了大量的信息资源，但由于这些数据分别由相互孤立的系统产生和管理，在信息采集过程中大部分依赖于手工方式，各单位之间独立采集的数据很难相互核对，误差很大，因而存在信息重复采集、数据矛盾、标准不统一的现象，给信息资源共享带来了很大的困难。以信息化发展较快的某市 A 为例，在近期流动人口数据汇集中，计生部门与公安部门首次数据的比对就有 69 万人的误差。再如某市 B，公安人口管理系统和社会保障管理系统的建设都涉及人口基础信息的采集，也存在二者之间数据矛盾的现象[125]。

3．对合作过程的不信任

在电子政务业务中，出现对合作对象不信任的现象主要表现在政务信息资源共享和交换过程中的共享效益不明显，信息提供方担心在信息资源共享过程中自身的利益受损或权力下降。其中，一些业务部门围绕需求开发了不少相关的政务信息资源，如企业基础信息、人口基础信息和空间基础信息等，但由于其在开发过程中花费了大量的人力、财力，目前仍在对一些项目进行收费。如果无偿把这些信息资源拿出来共享，又没有补偿机制，势必会影响其积极性。这正如 Dawes 在其政府部门间信息资源共享收益与风险模型中所指出的（Dawes，1996），组织对信息资源共享的预期收益和预期风险将影响和形成组织间信息资源共享的实际经验，然后对政府组织间信息资源共享的政策和原则形成指导并循环作用。所以说，组织成员的“预期效果”在一定程度上影响着对电子政务信息资源共享的态度。

因此，加强信息安全保障能力、建立健全信息资源管理机制将能够有效解决电子政务信息资源共享工作中面临的组织间的信任缺失问题。

4.4.4　共享环境因素间接影响共享的感知收益

共享环境因素间接影响共享的感知收益，因此也必须给予重视。这表现在法

[125] 顾德道，高广耀．宁波市政务信息资源共享管理对策分析[J]．信息化建设，2008（31）.

律法规建设、技术标准的推进和监督评估机制的完善等都是推动电子政务信息资源共享工作的积极因素。

1．法律法规对电子政务信息资源共享的作用和影响

法律法规在电子政务信息资源共享中能够明确权责关系，并以法律法规的形式规范信息资源共享的内容、方式和责任，进而完善信息资源共享制度，以此推动和促进信息资源的流动和传播。在我国电子政务实践中，国家和地方相继制定和颁布了电子政务信息资源共享建设相关的法规和文件，这些法规和文件就加强组织领导、建立信息资源共享工作机制和重点工作任务等做出了规范，有效指导了电子政务信息资源共享工作的实践。

2．标准规范对电子政务信息资源共享的作用和影响

标准化是电子政务建设的基础性工作，能够将各个业务环节有机连接起来，为信息资源共享提供技术准则。标准化具有协调和优化电子政务信息资源共享的作用，能够提高信息资源共享的效率，提高信息系统的安全性、可靠性。由于跨部门信息资源共享涉及信息的多样性、技术的多样性等，制定和颁布相关技术标准能够解决因信息采集和加工过程中的编码、格式、电子文件格式、网络通信协议等不一致为共享带来的困难。在我国电子政务实践中，国家和地方相继制定和颁布了涵盖信息资源共享的数据标准、网络技术规范、应用服务标准等一系列相关标准。这些标准在电子政务信息资源共享建设的实践中起到了规范建设的作用，在一定程度上促进了共享的规范实施。

因此，在电子政务信息资源共享建设中不应忽视环境因素对收益的影响作用，应积极建立健全法律法规环境，制定全面、合理的标准规范体系，有力地推动电子政务信息资源共享建设。

4.5　电子政务信息资源共享的安全风险及成因分析

研究表明，信息安全问题已成为阻碍电子政务信息资源共享深入推进的重要

瓶颈。在电子政务信息资源共享过程中，随时可能面临各种各样的威胁，如计算机故障、病毒感染，以及遭遇黑客入侵导致信息泄密、篡改等，主要安全风险表现在以下几个方面。

4.5.1　网络泄密成为电子政务信息资源共享面临的首要威胁

政务信息涉及国家秘密、商业机密及个人信息，关系到政府部门、重要系统的安全和社会稳定。信息资源共享加大了政务信息资源的开放性，放大了信息被非法利用的风险，如何降低泄密风险成为电子政务信息资源共享面临的首要挑战。

一是“政务敏感信息”的界定、分类不清楚，在难以区分信息敏感级别的情况下，很难保证敏感信息不遭泄露。在我们调研的 95 家单位中，仅 21%的单位认为相关政策对“什么样的信息可以共享”做出了明确规定，仅 28.4%的单位能保证共享的信息不被伪造或篡改。

二是信息资源共享的责权机制不明确，带来了“出了泄密事件谁担责”的问题，在这种情况下，有关部门往往会选择少共享或不共享，这成为阻碍电子政务信息资源共享的重要原因之一。

三是管理机制不完善容易造成重要信息资源的人为或无意泄露。信息资源共享需要多部门合作，在共享过程中如果缺少完善的管理机制，则很容易给不法分子可乘之机。在调查“谷歌地球”涉嫌曝光我国军事机密的事件时发现，“谷歌地球”的基础数据来源于我国政府机构，服务器却在美国，我国没有管辖权，我国党、政、军重要数据安全面临严重威胁。

4.5.2　个人隐私泄露形势严峻

在当今信息化社会，个人隐私权的主要内容已由原先的个人私事，发展到包括个人偏好、通讯记录、疾病记录、性格倾向、信用记录、违法记录、雇用信息等在内的系列信息。随着电子政务互联共享的深入推进，大量个人信息被纳入政

府数据库中。如此丰富的个人数据一旦被泄露，后果将不堪设想。

一是大量个人信息的数字化、集中化管理加大了隐私泄露风险。在信息资源共享的网络环境下，大量的个人信息随时都有可能被非法窃取、传输、使用，甚至利用个人信息进行犯罪活动，公民的隐私权正处于深刻的危机边缘。

二是个人隐私权保护的立法滞后。我国有关电子政务中个人隐私权保护的立法层次较低，法律条文过于笼统，缺乏可操作性，对个人隐私权的保护还处于较低水平，无法充分、有效地协调信息资源共享与隐私保护之间的冲突。对收集个人数据的依据、收集个人数据的程序、个人数据的使用及安全、本人对数据拥有的权利、侵害数据的法律责任都缺乏相应的规定，亟待明确。

三是缺乏个人隐私泄露的技术防护措施，加之政府对个人隐私泄露可能造成的后果缺乏充分估计，往往引发意想不到的社会问题。天涯社区 4000 万用户资料泄露，网易、当当网、开心网、CSDN 社区等也不同程度地发生了用户资料泄露，给几千万网民带来了个人隐私甚至是银行账号安全的威胁，引起了广泛的社会关注和恐慌情绪。

4.5.3 新技术应用带来的安全问题

大数据、云计算、移动通信、物联网等新技术的应用助力电子政务信息资源共享工作取得新突破，但同时也带来了新的安全风险。

一是信息存储安全问题。以政务共享平台中普遍推广的云计算为例，目前云计算高端技术主要受 Microsoft、IBM、Amazon、Google 等国外 IT 巨头掌控，无论是技术还是管理都存在极大的不可控性，这样的基础平台很难保障政务信息的安全可控。

二是信息采集安全问题。物联网作为信息采集终端在电子政务领域广泛应用，可能从源头上带来信息安全问题。目前，我国政务领域已开始应用物联网传感技术采集交通、环境、地理位置等基础数据，但我国目前从事传感器生产的 95%都是小企业，且 90%以上都是代工生产，技术水平较低。另据工业和信息化部电信

研究院《物联网白皮书（2011）》显示，国内中高档传感器几乎 100%从国外进口，90%的 RFID 芯片依赖国外，智能电网核心芯片几乎全是国外产品，智能处理和云计算的基础架构均由发达国家主导。这些新技术的推广应用会对国家关键信息设施带来潜在的安全隐患。

三是终端安全问题。移动通信在政务领域的应用增加了信息丢失或泄露的风险。法国政府就以黑莓手机容易让伺服器所在的美国窃取情报为由，禁止政府高官使用。

第 5 章
电子政务信息资源共享的安全保障机制建设案例研究

新时期我国十分重视电子政务信息资源共享和信息安全保障工作。在国家有关政策的指引下，一些省市，如北京、上海、江苏、江西、广东等在电子政务信息资源共享和信息安全保障机制建设方面做了很多有益的探索。本章选取了江苏、江西两个省和一个省会城市广州为案例，对这三个省（市）2002—2010 年的电子政务信息资源共享安全保障机制进行研究分析，旨在归纳我国地方电子政务信息资源共享安全保障机制建设的一些成功经验，提炼出可在全国推广的普遍性对策。

5.1 理论假设

在第 2 章，我们分别从系统学、信息经济学和管理学等角度对电子政务信息资源共享与安全保障的基础关系做出了分析。在此基础上，提出案例研究的基本理论框架如下（见图 5-1）。

H1：共享效益的显现推动组织开展政务信息资源共享工作，是形成良性循环的重要动力。

H2：重视信息安全保障工作，是电子政务信息资源共享获得成功的基础。

H3：电子政务信息资源共享与信息安全，看似相互对立，实则相互促进。二者之间的关系在实践中的表现是：以安全保障共享，以共享促进安全。

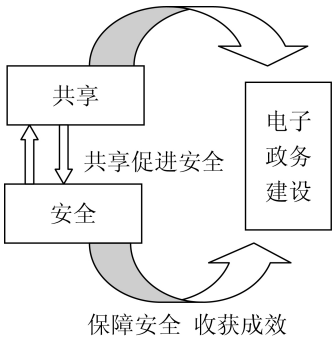


图 5-1 案例研究的理论框架

5.2 方案设计

5.2.1 案例选择

案例研究的首要任务是进行案例选择。Yin 提出案例研究是非抽样的研究，

理论研究和目的抽样是要结合运用的[126]。根据本章的理论框架与研究目的，在案例选择上，遵循以下标准：① 所选案例的电子政务信息资源共享建设在全国处于较为领先水平；② 在选择中考虑地域分布的代表性；③ 全部案例在电子政务信息资源共享的安全保障机制建设中具有典型性。Eisenhardt[127]、Yin 等学者指出，在有条件的情况下，可以选择开展多案例研究，以使研究结果更具说服力。Sanders[128]则认为，进行多案例研究时案例数目最好为 3～6 个。基于上述学者的建议，结合本研究所掌握资料的情况，我们采用了多案例研究方法。研究中采用了三个案例，选择了电子政务信息资源共享工作突出的江苏、江西两个省，以及省会城市广州来开展研究。三个案例的基本信息如表 5-1 所示。

表 5-1　三省（市）基本信息

省　名 数 据 项	江苏（省级）	江西（省级）	广州（副省级）
面积（平方公里）	102 600	166 900	7434
人口（万人）	7700	4457	1200
2010 年地区生产总值（亿元）	40 903	9435	10 604
2010 年基础设施投资（亿元）	3304	5545	3263
互联网普及率（截至 2010 年年底）	42.8%	21.4%	71.1%

数据来源：省（市）政府网站、CNNIC 等。

5.2.2　效度与信度分析

1．研究问题的确定

本案例研究旨在通过电子政务信息资源共享建设的案例研究，分析和归纳出

[126] Yin R. Case study research – design and methods [M]. 2nd ed. Thousand Oaks : Sage Publications, 1994:98-100.

[127] Eisenhardt K.M. Better stories and better constructs: The case for rigor and comparative logic [J]. Academy of Management Review, 1991, 16(3):620-627.

[128] Sanders P. Phenomenology: Anew way of viewing organizational research [J]. Academy of Management Review, 1982, 7(3):353-360.

电子政务信息资源共享安全保障机制建设的一些成功经验，进而提炼出可在全国推广的普遍性对策。

本案例研究的参与者都是从事电子政务和信息安全方面的研究人员，具有一定的研究经验，在围绕研究问题阅读了大量文献资料后，确定出基本的研究框架，经过反复讨论之后确定了所要研究的问题及思路。在确立研究问题的基础上，根据案例研究对象的选择标准，筛选研究对象，整理相关资料，进而开展案例研究工作。

2．资料收集

在案例分析中，有访谈、文献研究、档案记录、直接观察、实物证据和参与性观察 6 种证据来源。为保证每个案例的构建效度，我们根据研究问题来确定证据的类别，分别是访谈记录、内部档案记录和相关文献、相关新闻报道，从而构成案例中的证据三角。

3．资料整理的效度与信度

在访谈记录方面，我们走访了相关省市电子政务建设方面的相关负责人员，在访谈开始前准备了开放性的问题提纲。在每次访谈过程中都有两位以上的研究人员参与其中，以保证访谈过程有效。此外，为提高研究的信度，在访谈过程中我们注重根据实际情况进一步挖掘信息形成完整证据链的工作。在访谈结束后，由参与访谈的相关研究人员对访谈记录进行整理，对信息不清晰和理解不一致的部分进行讨论，通过反复讨论和查找相关资料进行求证来最终达成共识，以此保证资料分析过程中的效度与信度。

在内部档案记录和相关文献方面，我们得到了相关部门的大力支持，查阅了相关的档案记录；在中国期刊网的数据库中查阅了大量相关资料，并购买了相关的书籍阅读。这些权威性的内部档案记录和公开发表的文献、书籍，保证了研究资料的效度与信度。

在相关新闻报道方面，我们密切关注各地政府信息化部门的官方网站及电子政务建设相关的权威网站，从中获取权威的动态信息，以保证新闻报道资料获取的效度与信度。

5.3　案例分析

5.3.1　三省（市）电子政务信息资源共享建设情况

江苏省电子政务信息资源共享建设规划较早，并且得到了领导的高度重视。2002 年，江苏省为电子政务建设设立的目标就包括“建设标准统一、结构合理、功能完善、安全可靠的政务信息网络平台”、“推进政务信息资源库建设”、“使信息资源共享程度显著提高”、“实现重点业务系统互联互通”。江苏省以“一把手”工程推动电子政务建设，省信息办和市信息办分别主管省市的电子政务信息资源共享工作，许多地级市成立了以市长为组长的信息化领导小组和以分管领导任组长的电子政务建设协调指导小组，统筹电子政务信息资源共享建设的重大方针政策，组织、协调各地电子政务重大项目和重点工程建设。全省电子政务行政主管部门明确要求加强资源整合共享，以统一标准进行资源整合和共享。2004 年年底，江苏省电子政务内网平台搭建成立；2005 年年底，江苏省电子政务内网门户网站正式开通；2005 年 8 月，在电子政务内网建设了电子政务交换平台，实现了省市县三级政务、各省级机关共 400 多家单位之间的数据交换和内部公文流转；2006 年 6 月，通过“江苏省信息系统信息资源共享平台”连通了 13 市并制定了《江苏省信息系统信息资源共享平台考评细则》；2006 年年底，江苏省电子政务外网建设完成；此外，还建立了人口、法人单位、自然资源和空间地理、宏观经济 4 个基础数据库，规划了包括办公业务资源系统、金融监管工程、社会保障工程等在内的 17 个业务系统，实现了统一的信息资源共享平台、统一的应用系统整合平台、统一的信息安全保障平台的内网平台“三统一”。江苏省积极探索区域信息资源共享协作机制，与上海、浙江共同建立了“长三角”信息资源共享制度，按照业务需求建立了政务专业领域的信息资源共享平台，推动了区域共享互利。

江西省在电子政务信息资源共享模式上独具特色，全省电子政务建设按照“集中统一、整合共享、联合协同、安全高效”的原则来推进，坚持以“统一网络平台”和“统一交换平台”为基础来解决信息资源共享的条块分割和部门割据问题。

2004 年年初，江西省开通了覆盖省、11 个市、109 个县三级党政机关的全省电子政务统一网络平台，三级网络分别横向连接本级党委、人大、政府、政协和各直属部门，并实现省、市、县三级对口部门纵向联网，江西省的省、市、县三级政务信息网网管中心提供网络平台的互联网出口服务。近几年，江西省又通过建设“政务网乡乡通工程”，实现省、市、县、乡四级“一网通”。另外，江西省率先完成了国家电子政务外网江西分中心建设。目前，在江西省统一网络平台（包括内网和外网）上，已经承载了 800 多个应用系统，其中省级承载了 200 多个应用系统，市级承载了 100 多个应用系统，县级承载了 500 多个应用系统。2010 年，江西省建成了覆盖省、市、县三级政务部门的全省公共数据统一交换平台，实现了全省跨部门、跨地区、多业务、异构系统、异构数据库之间的信息交换和共享。江西省通过整合电子政务应用，建设电子政务统一网络和统一交换平台，既提高了政务信息资源利用的效率，又保障了电子政务系统和网络的安全。

广州市作为全国经济最发达的城市之一，拥有全国领先的信息化基础设施，计算机网络在政府部门中普及率高，为政务信息资源共享创造了良好的基础环境。广州市的政务信息资源共享不是按照统一规划的蓝图自顶向下推进的，而是按照业务领域的需求，以“业务圈”的形式组织共享，以业务效益驱动。2003 年，广州市依托 14 个市级部门和 12 个区（县级市）启动了大社保项目“广州市社会保障信息系统”，社保信息整合与共享大大改善了社保工作，创造了业务效益，其成功不仅带动了工商、人口管理、医保等领域的信息资源共享需求，还为构建全市电子政务数据中心打下了基础。基于此，广州市信息办建立了广州市电子政务数据中心，以“一数一源”、“依申请提供，依职能使用”、“有限规模”、“灵活处理”为原则，以业务需求为导向，以业务效益为驱动，以提高政务业务管理与服务能力为目标，围绕具体行政业务，在相关部门与市电子政务数据中心之间建立了信息资源共享平台，加上全市自然人、法人单位基础数据库的建设，配合《广州市政务信息资源共享管理办法》的贯彻，切实加快了资源共享、系统整合、条块结合、业务协同的步伐。目前，广州市已建成了政府信息化的物理基础平台，开通了公共数据平台，优化了公共网络平台、公共应用平台和公共服务平台，一些部门利用这些平台建立起跨部门业务系统联动机制，全市电子政务从行业（部门）业务应用系统逐步进入跨行业、跨部门信息应用系统的整合和提升阶段。

三省（市）对于电子政务信息资源共享及其信息安全建设都出台了相关政策文件。表 5-2 分别从电子政务建设生命周期的规划、建设、运行、评估、安全等环节进行了举例。

表 5-2　三省（市）支持电子政务建设的政策文件（举例）

省（市）名 / 阶段	江苏省	江西省	广州市
规划	《江苏省政府办公厅关于进一步推进全省电子政务建设的意见》（苏政办发〔2007〕8 号）	《中共宜昌市委、宜昌市人民政府关于加快推进电子政务建设的意见》	《关于加快电子政务建设提高政府行政效能和公共服务能力的工作意见》（穗府办〔2006〕36 号）
建设	《无锡市电子政务建设实施方案》（锡政办发〔2004〕30 号）	《江西省人民政府办公厅关于印发江西省网上审批和电子监察系统建设工作方案的通知》（赣府厅字〔2009〕16 号）	《广州市人民政府办公厅印发加快全市电子政务建设工作方案的通知》（穗府办〔2010〕41 号）
运行	《江苏省人民政府办公厅关于加强政府系统电子政务管理工作的通知（苏政办发〔2009〕98 号）》	《江西省电子政务建设项目管理暂行办法》（赣发改高技字〔2007〕1334 号）	《关于加强资源整合提高我市电子政务综合效能的意见》（穗府办〔2006〕6 号）
评估	《江苏省省级机关电子政务项目绩效评价办法》（苏信息办〔2008〕15 号）	《江西省政府网站绩效评估办法》（通过评审）	《广州市电子政务绩效评估管理办法》（穗信息化字〔2007〕61 号）
安全	《江苏省电子政务内网安全保密产品推荐目录》、《江苏省电子政务内网接入审批暂行办法》	《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（赣发改高技字〔2008〕1363 号）	《广州市电子政务网络信息安全应急处理流程规范（试行）》

5.3.2 基于共性的分析

1. 通过信息资源共享能够节约社会成本、提高服务效率

实践证明，政务信息资源共享及基础设施共建共享为社会节约了大量资源。一方面，跨部门信息资源共享活动为国家、社会带来显著的经济效益。信息资源共享带来的经济效益最典型的表现是在治理偷税漏税问题上。我国开展跨部门信息资源共享后，在第一次工商部门与税务部门的数据比对中，仅北京、杭州和深圳三个城市就发现有 37 838 户企业未按规定办理税务登记，如果按每户每月缴税 5000 元计算，每年可为国家收回税收损失 22.7 亿元。广州市在 2008 年工商局和税务局进行企业信息资源共享中交换信息 3.4 万条，发现未办理税务登记企业 1.7 万多家，经税务部门催办，全市的企业税务登记率超过 94%，为国家收回了大量损失。江苏省在第一次工商、税务、质监、海关等部门的企业信息比对中，对应率不到 60%，信息孤岛造成的损失可想而知。另一方面，基础设施共建共享有助于节约社会成本。2008 年 9 月底，工业和信息化部下发《关于推进电信基础设施共建共享的紧急通知》，全国全面启动共享共享工作，从 2008 年 10 月到 2010 年年底，全国共节约投资超过 200 亿元，江西省节约投资 11.8 亿元，江苏省节约投资约 6.5 亿元。

政务信息资源共享改进了业务流程，提高了政府部门为公众服务的效率。以广州为例，在未进行政务信息资源共享时，曾出现在发放越冬补助时，一位困难户同时收到来自不同部门的 22 条补助棉被的现象。2007 年江苏省公安机关依托政务信息资源共享平台，开展警务信息智能比对，发现违法犯罪线索 24.11 万条，破案约 11 万起，抓获各类在逃及布控人员 3.8 万名。江苏、江西、广州都通过信息资源共享显著改善了政府部门对税务、医疗、社保、就业、计生、教育、流动人口管理等方面的综合管理，增强了政府的公共服务能力，推动了服务型政府构建。

经济效益和社会效益推动信息资源共享不断扩展。广州市政府自 2003 年开展社保信息资源共享项目取得成功后，更多政府部门申请加入相关领域的信息资源共享，数据整合日益深入。信息资源共享取得的效益推动电子政务信息资源共享

进入良性循环，共享效益成为业务单位积极参与信息资源共享的重要动力。

2．信息安全工作保障电子政务信息资源共享平稳开展

共享信息的安全保密是电子政务信息资源共享的前提和基础。三省（市）都通过有效的信息安全保障措施为政务信息资源共享工作创造良好环境。

首先，战略层面进行布局。江苏省在 2002 年省政府办公厅发布的《江苏省电子政务建设指导意见》（苏政办发〔2002〕126 号）中提出，要“建立电子政务网络与信息安全保障体系，加快电子政务信息安全产品的研制与开发，逐步完善安全管理体制，建设全省电子政务 CA 认证中心，建立应急支援中心和数据灾难备份基地”。江西省实行电子政务安全系统与主体工程“同步规划、同步建设、同步发展”的原则，通过重点保护基础信息网络和重要信息系统、加强互联网监测治理、健全应急响应制度、强化灾难备份建设、加快信息安全人才培养等来推进政务信息资源共享安全保障工作。广州市人民政府办公厅发布的《加快全市电子政务建设工作方案》（穗府办〔2010〕41 号）指出，要“建立和实施全市电子政务安全态势和风险评估机制，建设全市统一的安全认证体系和容灾备份体系”。

其次，领导层面加以重视。三省（市）都有专门负责电子政务信息安全保障工作的部门和责任领导。如广州市政府指定市科技局和信息化局会同市公安局、国安局、保密局共同完善电子政务信息安全基础设施和信息安全保障体系。

再次，管理机制有效跟进。江苏省先后制定了《江苏省电子政务内网保密管理暂行规定》、《江苏省电子政务内网安全保密解决方案》、《江苏省电子政务内网安全保密产品推荐目录》及《江苏省电子政务内网接入审批暂行办法》等文件，全省各地市也纷纷出台地方有关网络安全的规范、标准，例如苏州市出台了《苏州市电子政务网信息安全规范》、《苏州市电子政务网网管平台规划、规范》、《苏州市电子政务网、社区网建设标准》等标准和规范。

最后，技术保障落到实处。江西省成立了 CA 认证中心，统一推进全省电子认证服务，用“一证通”的方式解决了全省电子政务安全认证。江苏省从 2002 年开始规划建设的电子证书认证系统于 2005 年年底获得了《电子认证服务使用密码许可证》和《电子认证服务许可证》，具备了电子认证的法律条件，电子政务

CA 认证已应用于财政等部门。以政务信息资源共享为主题的江苏省宏观经济管理系统从物理层、网络层、应用层、容灾备份、安全审计、安全管理制度等角度构建了信息安全防护体系。

从另一个角度来看，政务信息资源共享的深入推进又促进了信息安全保障体系的建设完善。

一是政务信息资源共享对信息安全保密的要求更高。政务信息资源具有不同程度的敏感性和保密性，如果发生泄露或被不正当利用，则会对国家安全、社会稳定、国家财产构成严重威胁。2010 年网络泄密案占全国泄密案的 70%，网络失泄密的文件资料达 70 万份。据国家互联网应急协调处理中心监测，我国约 60%的部委级网站存在不同程度的安全隐患，这对电子政务信息资源共享工作的深入开展带来巨大的安全风险。另外，政务信息资源共享给公民和企业带来了个人隐私和商业秘密泄露风险。电子政务信息资源共享依托的人口、法人、地理空间等基础数据库和“金字工程”等涉及大量敏感信息，一旦共享不当造成公共或个人数据泄露，就会侵犯公众利益，引发治安和法律纠纷。

二是政务信息系统自主可控的要求更迫切。电子政务信息系统与电子政务系统的一大区别在于，政务系统大多是关乎国计民生的重要系统，承载的信息资源关系到国家安全命脉，因而对自主可控有更高的要求。我国电子政务信息系统的核心软硬件、系统集成、关键设备和安全服务严重依赖国外厂商的局面没有得到根本改变。据统计，国内 70%的信息设备来自国外，我国电子政务系统中微软、IBM、HP、思科、甲骨文等国外软硬件仍占主流，电子政务工程采购的软硬件产品中，自主品牌产品采购金额还不到采购总额的 4 成。关键芯片、操作系统严重依赖国外的局面导致政务信息系统的潜在安全风险突出，急需信息安全保障技术创新。

三是信息资源共享中的新技术应用对信息安全保障体系提出新内容。近年来，云计算、物联网等新技术在电子政务领域的广泛渗透，移动政务快速发展，新技术应用给数据存储、传输和用户隐私等带来了新的安全风险，这些新技术的安全防范措施需得到及时跟进，以免给政务系统造成新的安全隐患。

5.3.3　基于个性的分析

三省（市）在信息资源共享的安全保障工作上拥有各自的特色，取得了一定的经验和成效（见表 5-3）。

表 5-3　三省（市）加强电子政务信息资源共享安全保障的典型做法

省（市）	典型做法
江苏省	• 建设统一的信息安全保障平台 • 建立电子政务 CA 认证中心，开通长三角数字证书互认平台
江西省	• 对电子政务网络的互联网出口服务实行统一管理 • 在信息资源共享和交换平台中大规模使用国产基础软件
广州市	• 分为“共享数据”和“交换数据”分别监管 • 信息资源共享时灵活使用状态数据替代敏感数据

1．区域信息资源共享合作模式有利于区域经济发展

江苏省与上海、浙江等地建立了信息协商联席会议制度，每年定期召开会议，磋商电子政务发展有关事宜，建立跨区域信息沟通和预警通报机制，促进区域经济共同发展。2009 年，江苏省 13 个市共同成立了江苏省区域电子政务信息安全联盟，研究电子政务信息安全保障机制、信息安全产品选用准入机制等。2010 年 12 月，苏、浙、皖、沪三省一市成立了“长三角电子认证服务联盟”，启动了“长三角数字证书应用互联互通平台”，逐步打破了电子认证服务局限于单个地方、单一行业、单一部门业务应用的局面，为税务、工商、社保、质监、统计、医疗、海关、招投标等几十项电子政务业务协同应用提供了有力的安全保障，推动了区域一体化的网络信任体系建设，充分发挥了电子认证的基础性作用。探索区域性电子政务信息资源共享新模式，服务于区域经济发展。另外，调研了解到珠三角、环渤海湾等区域在区域电子政务互联互通、信息资源共享工作上也进行了有益探索。区域信息资源共享作为省内信息资源共享的延展，有助于进一步打破信息孤岛，充分发挥信息资源共享的区域经济和社会效益，推动信息资源共享在全国范围内实现。表 5-4 列举了长三角推动跨区域政务信息资源共享的部分协议。

表 5-4　长三角推动跨区域政务信息资源共享的部分协议

日　　期	协议名称	主要内容
2008-9-11	苏、浙、沪工商行政管理共同签署《苏、浙、沪工商行政管理局公平交易（经济检查）执法协作协议》	设立省际公平交易（经济检查）执法协作信息专栏，通报大案要案，交流办案经验，分析研究对策，实现信息资源共享
2008-10-23	苏、浙、沪政法委共同签署《长三角地区政法综治协作交流框架协议》	整合三地流动人口信息资源，建立三地人口管理网络平台，并依托劳动保障部门，推进三地企业劳动用工信息资源共享
2008-10-24	苏、浙、沪高院共同签署《长江三角洲地区人民法院司法工作协作交流协议》	规划建立执行案件信息资源共享平台，共享被执行人在长三角区域所涉案件的数量、其可执行财产的分布等重要执行资源

2．关键核心设备国产化能够进一步确保信息安全

目前我国许多电子政务系统、平台及关键业务应用都建立在非国产的、非自主可控的基础软硬件上，这对于保障电子政务信息安全是一个突出问题。近年来，我国一直非常重视核心技术和产品的国产化，把“核心电子器件、高端通用芯片及基础软件产品重大专项”确立为推进信息技术发展的 16 个重大专项之一。江西省在电子政务建设中大规模采用国产基础软件，提高了政务系统的自主可控能力。主要做法包括：选择与国内公司共同申报国家电子政务应用示范项目，以国产基础软件为支撑建立示范应用；与国产中间件厂商合作开发电子政务应用软件，利用国产具有自主知识产权的安全操作系统、安全数据库、安全中间件和服务器、安全接入设备等，建立江西省电子政务统一应用平台；在全省广泛应用国产基础软件，构建省级政务共享数据中心、数据交换中心、网上服务中心、安全管理中心和灾难备份中心。江西省通过实践证明，国产基础软件不仅达到了电子政务核心应用的安全设计要求，并且经济实用、服务周到，许多产品的价格比国外同类产品低好几倍，且对客户服务的响应优质高效。

3．对敏感数据分类有助于推动电子政务信息资源共享

广州市通过对政务敏感信息进行分类开展信息资源安全管理。广州市社会保障信息系统将可共享的政务信息分为两类：一类是共享数据，主要是基础数据，这类数据由电子政务数据中心统一管理，数据中心对数据进行比对与核实，保证

数据质量，其信息资源共享统一通过数据中心进行；另一类是交换数据，属于业务数据，存于各部门业务系统，数据中心不负责质量管理，可通过数据中心交换平台进行对应交换。对共享信息进行分类管理的做法明确了各方责任，有助于确保电子政务信息资源共享活动安全、有序开展。广州市对敏感信息处理的另一项做法是用状态数据替代敏感数据。有些政务信息不便于按原样提供共享，广州市确立了“灵活处理”的原则，在满足业务需求的情况下，使用状态数据（如“已纳税”）或区间数据（如“高收入者”）代替精确数据（如“纳税额”）提供共享，一方面降低了数据提供方的责任风险，减少了信息资源共享的阻碍；另一方面尊重了个人隐私，保护了商业秘密，也确保了信息安全。

5.3.4　存在的问题

三省（市）在政务信息资源共享方面都进行了积极探索，取得了较好的应用成效，但也反映出一些问题。

1．指导性原则缺失

从 2002 年中办发 17 号文提出要信息资源共享以来，我国电子政务信息资源共享工作已开展十余年，而国家层面的战略性、指导性管理办法或条例却迟迟不出台。目前，三省（市）中仅广州市研究公布了《广州市政府信息资源共享管理规定（草案）》，江苏省南京市出台了《南京市政务信息资源共享管理办法（试行）》，江苏省、江西省都未出台省级的政务信息资源管理办法。法律的滞后使得信息资源共享中出现的隐私保护、商业秘密保护等问题没有明确的法律依据，造成相关部门责任不清，阻碍了信息资源共享。

2．国家标准滞后

标准化是电子政务建设的基础性工作。《国家电子政务总体框架》指出，标准化体系是电子政务建设和发展的基础，而我国政府部门在开展信息资源共享和业务协同时却遭遇了标准不统一的制约。一是地方标准与国家标准不统一。以地理信息数据标准为例，各部门采用的地理信息数据标准与国家基础地理信息标准不一致，给地理信息共建共享带来阻碍。二是各业务部门间对数据资源的定义、表

述不同。各地的应用部门，甚至同一地区存在多套标准，如青岛市就有三套地理坐标，开展跨部门共享时还需进行数据格式的转换。我国的电子政务建设往往是各省市先行试点，等应用比较成熟了国家再统一出标准，各省市又要按照国家标准进行重建，不仅造成资源浪费，还影响了电子政务发展进程。

3．信息安全问题成为瓶颈

自 2008 年起，工业和信息化部每年主办全国地方电子政务信息资源共享和业务协同经验交流会，各省市代表分析信息资源共享情况，其中信息安全风险和隐患等问题成为信息资源共享的一大阻碍。由于信息资源共享的安全得不到有效保障，一些部门常常因“涉及安全问题”无法从其他部门共享信息，有些部门甚至以保密为由拒绝提供共享，许多部门在面对“什么能共享、什么不能共享”等问题时无从下手。对于化解信息安全风险和隐患的方法，本案例研究中江苏、江西、广州三地都针对自身特点，对政务信息资源共享的信息安全保障措施进行了积极探索，但由于各地电子政务建设情况不同，一些地方取得的先进经验难以在全国范围进行推广。当前，信息安全风险成为严重阻碍信息资源共享工作深入推进的瓶颈。

5.4 案例研究的结论

通过案例研究，在验证理论假设的基础上，得出以下结论。

1．电子政务信息资源共享和信息安全工作突出的组织，普遍有比较健全的领导体制，有长远的战略规划部署

健全的领导体制和全局性的、长远的战略规划部署是电子政务资源共享建设卓有成效的必备要素。江苏、江西、广州三省（市）在电子政务信息资源共享和信息安全保障方面都制定了长期的战略规划，主管部门高度重视，积极贯彻落实中央有关精神，在国家统一的战略部署下，形成了具有地方特色的电子政务信息资源开发利用的领导体制。如江苏省成立了江苏省信息化工作领导小组、江苏省政务公开领导小组、江苏省电子政务建设协调指导小组，统一领导、推进全省的

政务信息资源共享工作。各部门为了有效推进本部门的政务信息资源共享，也成立了相关的领导小组，如江苏省农村党员干部现代远程教育领导小组、江苏省文化共享工程领导小组等。

2．信息安全保障体系建设和完善是化解和消除政府组织共享忧虑的一个重要因素，对信息资源共享工作的顺利开展具有积极的推进作用

组织间的信任是实施电子政务信息资源共享极为重要的软环境，如果缺失，将严重制约着电子政务信息资源共享，导致组织间感知的扭曲，成为瓶颈性的风险因素。在电子政务信息资源共享中，政府机构之间、政府与公众之间、政府与企业之间信任关系的建立，是电子政务得以推广应用的关键，是实现信息资源共享和跨部门、跨地区协同办公的基础。当前，电子政务信息资源共享中组织成员的“预期效果”在一定程度上影响着对电子政务信息资源共享的态度。信息安全保障体系的建设和完善，有助于使组织成员的“预期效果”与信息资源共享的实践效果达成一致，有助于提高组织间的信任，是化解和消除政府组织共享忧虑的一个重要因素，对信息资源共享工作的顺利开展具有积极的推进作用。

3．电子政务信息资源管理中心和交换中心是信息资源共享工作得以顺利进行的基础性平台

电子政务信息资源共享中涉及大量的信息资源，这些信息资源中包含政府机密、涉及国家安全，信息资源的管理工作任重而道远。建立健全电子政务信息资源管理中心能够统一协调和有效管理政务信息资源，使得信息资源共享工作得以顺利进行。作为服务平台的交换中心，根据政务信息资源目录体系向信息使用者提供政务信息查询、检索和定位，并在规定的安全机制下，通过交换体系获得信息资源，向信息使用者提供信息访问服务。电子政务信息资源管理中心和交换中心作为两大基础性平台，为电子政务信息资源共享工作的开展打下了良好基础。

4．效益的凸显是政府组织开展电子政务信息资源共享和信息安全保障工作的动力源泉

信息作为现代社会的一种重要资源，在其他信息活动要素（如技术、设备、

资金、人等）的支持下，能够为人类创造珍贵的物质财富和精神财富。电子政务信息资源共享能够提升经济效益和社会效益，其中，经济效益是驱动力，社会效益则是落脚点。经济效益体现在降低信息收集成本、提高组织运行的效率等方面；社会效益主要体现在信息资源共享后给人民生活带来的便利及对社会经济发展的促进作用。案例研究的结果表明，江苏、江西、广州三省（市）作为电子政务信息资源共享和安全保障工作开展较好的地区，都是由于信息资源共享工作实实在在地提高了政府的工作效率，更好地为人民提供了公共服务，获得了社会各界的认可；反之，经济效益和社会效益的提高又进一步肯定了电子政务信息资源共享工作的价值和意义，成为推动电子政务信息资源共享的动力。

5．电子政务信息资源共享的信息安全制度建设是电子政务信息资源共享可持续、健康、良性发展的保障

对江苏、江西、广州三省（市）的研究表明，只有做好信息安全保障工作，才能放心地推进电子政务信息资源共享工作。电子政务信息资源共享必然带来诸多安全风险，这是因为信息资源共享涉及信息生命周期的每个阶段，面临着来自内部和外部的种种危险。政务信息资源共享环境下的信息安全保障更具复杂性，仅仅采用技术层面的保障不能满足电子政务信息资源共享安全保障的需求，安全的电子政务信息资源共享建设还应囊括管理层面的保障。以安全保共享，以共享促安全，相辅相成，只有建立健全电子政务信息资源共享的信息安全保障制度才是应对安全威胁和安全风险的重要手段，才能真正促进和保障电子政务信息资源共享可持续、健康、良性发展。

第 6 章
电子政务信息资源共享的安全保障机制构建

本章以前面章节的理论研究、政策比较研究和实证研究为基础，基于系统学方法构建了电子政务信息资源共享的安全保障机制理论模型，从战略、管理和技术三个基础保障要素入手，结合当前我国电子政务信息资源共享中遇到的信息安全难点和关键问题，以系统学的整体性、协同性、动态性安全观为指导，从宏观上设计建立了电子政务信息资源共享的安全保障机制。

6.1 理论基础和实践依据

6.1.1 理论基础

钱学森院士在 1995 年就指出：“信息网络加用户将构成一个‘开放的复杂巨系统’，不是简单巨系统，更不是大系统、小系统等容易调控的系统。”电子政务信息空间不仅自身具有开放的复杂巨系统的特征，而且本身又是与经济、社会发展密切相关的一个人机结合、人网合一的重要系统。因此，如何处理好电子政务信息资源共享的安全保障这样一个层次复杂、动态演化，“人”在其中扮演着主要角色的复杂系统的安全问题，需要我们运用新的思维和方法来研究分析电子政务系统这一研究对象的系统学特性。

① 复杂性。我国电子政务的服务对象是面向 13 亿公众的，这就决定了电子政务要满足在各种条件下的面向服务系统的访问需求。与此同时，由于很多接口需要与互联网相连接，加上节点之间运行的复杂性、系统的动态特性带来的模糊性，这些复杂性很难被精确描述。

② 层次性。系统运行涉及的层面很多，既涉及政府宏观决策层面，又涉及面向公众服务的层面；系统既要辅以处理各种社会危机的能力，又要实现党和国家政策宣传窗口的功效。

③ 开放性。电子政务系统是一个开放体系，它与外界有着信息、物质和能量的交流。电子政务系统的管理人员、访问人员，甚至是攻击者，都能够实时参与信息空间的各种活动，使得系统处于一个开放、不停运动的状态。

④ 博弈性。复杂性科学区别于其他建模方法的关键点在于承认系统中研究主体的主动性和动态性，并认为个体与环境（包括个体之间）的相互影响是系统演化的主要动力，通过主体和环境的相互作用，使得个体的变化带动整个系统的变化，从而把宏观和微观有机地结合起来。基于此考虑，我们将攻防双方在一定时空环境中的“博弈”关系作为重要的考察因素。

⑤ 与社会系统紧密耦合。电子政务系统涉及政治、经济、教育、医疗、住房保障、水利、通信、工业等方方面面，与社会生活的方方面面息息相关、联系紧密。

6.1.2　实践依据

通过第 4 章的实证研究我们了解到：① 电子政务信息资源共享的安全风险无处不在，遍布信息存储、传输、交换、处理的各个阶段；② 在拥有重要信息系统的部门中，病毒侵害、黑客攻击、失窃密、程序故障等安全风险成为政务信息资源共享中各利益方开展工作的一大障碍；③ 电子政务信息资源共享的安全保障不仅要保障信息资源的保密性、完整性、可用性等基础安全属性，还要保障电子政务信息资源共享中的可信性这一重要属性，可信性包括信息的可信性、网络的可信性，以及对合作组织的可信性等方面。组织间的信任缺失，将严重制约着电子政务信息资源共享，导致组织间感知的扭曲，成为瓶颈性的风险因素。

通过第 5 章的案例研究我们认识到：① 战略规划和顶层设计、技术和管理保障对于电子政务信息资源共享工作同等重要，是电子政务信息资源共享和安全保障工作成功的基础因素；② 管理制度建设，如领导体制、法律法规、标准体系、运行机制，是保障电子政务信息资源共享良性发展的关键环节；③ 重要技术基础设施建设，特别是信息资源管理中心、信息资源目录体系与交换体系、网络信任体系建设，是保障电子政务信息资源共享顺利实施的重要工作。

6.2　模型构建

基于系统学原理，首先对研究对象进行定性描述是有效的研究方法，即在状态空间和参量空间中用几何方法等定性手段加以研究。系统所有状态构成的集合称为系统的状态空间，也称作相空间。空间的每个点称为状态点或相点。对于电子政务信息资源共享的安全保障模型，将其设计为 5 个独立变量，即保障状态维

Z、保障目标维 O、保障机制（或保障要素）维 E、时间维 T，以及威胁维 D。这样，该状态空间就是一个维数为 5 的状态空间。以状态变量 Z、O、E、T 为轴支撑起来的集合空间，成为电子政务信息资源安全保障模型的状态空间，如图 6-1 所示。状态变量的每一组具体值(z,o,e,d,t)代表系统的一个状态或相。

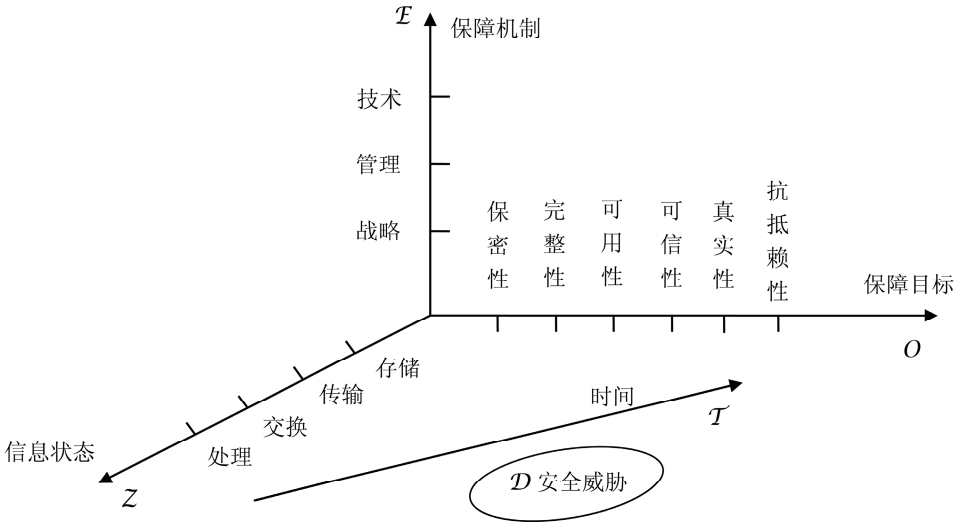


图 6-1　电子政务信息资源共享的安全保障机制理论模型

6.2.1　信息状态维

电子政务信息资源共享过程包括信息的存储、传输、交换和处理 4 种状态，且每个状态都涉及安全问题：信息在政务信息存储过程中可能被敌手所篡改，在传输过程中可能被截获，在交换过程中可能被泄露，在处理过程中可能被误操作。因此，电子政务信息资源共享的整个周期都面临着来自外部和内部的种种危险。

1．信息采集

信息采集包括对信息的收集和处理。政务信息采集时要保证信息的真实性和准确性。电子政务信息由直接接触该信息的权威部门进行采集。

2．信息存储

信息存储是指按照一定的格式和管理模式将信息资源保存到存储介质中。政务信息的存储要保证分类明确、安全可靠，便于社会充分利用已收集和加工所得的信息。

3．信息传输

信息传输是从一端将信息经信道传送到另一端，并被接收，包括传送和接收两个过程。政务信息传输要保证其有效性、可靠性和安全性。

4．信息交换

信息交换是电子政务的主要功能之一，是电子政务信息资源共享和协同的前提。信息交换要保证其实时性、可靠性和交换的效率。

5．信息处理

广义的信息处理就是对信息的接收、存储、转化、传送和发布等，狭义的信息处理是指信息的加工。信息加工是指通过判别、筛选、分类、排序、分析和再造等一系列过程，发掘信息的价值，使收集到的信息成为有用的信息资源。电子政务信息处理要做到操作规范、安全可靠。

6.2.2　保障目标维

电子政务信息资源共享不仅要求保证信息在存储、传输、交换和处理过程中的保密性、完整性、真实性、可用性和抗抵赖性，同时要求把信息系统建设成一个具有预警、保护、检测、响应、恢复和反击六大功能的纵深防御体系。1996 年美国国防部（DoD）在国防部令 S-3600.1 中对信息保障定义为：“保护和防御信息和信息系统，确保其可用性、完整性、保密性、真实性、抗抵赖性和可控性等特性。这包括在信息系统中融入保护、检测、响应，并提供信息系统的恢复功能。”对信息和信息系统安全属性的内涵和外延做出清晰界定，是实施安全保障等级划分的基础。从保障目标考虑，电子政务信息资源具有如下安全属性。

- 保密性（Confidentiality）：是指确保信息或信息系统提供的服务仅被已授权的人或系统访问。常用的保密性技术有密码技术、物理保护、防辐射等。
- 完整性（Integrity）：是指未经授权，信息不能被修改。从广义上讲，这里的信息不仅包括用户信息，还包括系统信息、操作系统的逻辑完整性和数据结构的一致性信息。完整性要求信息和信息系统的行为不被伪造或篡改。
- 可用性（Availability）：就是保证在需要的时候，被授权的实体可以访问信息、服务和相关的 IT 资源，甚至在信息系统部分受损或需要降级使用时，仍能为授权用户提供有效服务。
- 可信性（Trustbility）：就是保证在信息资源共享各个环节中保持对信息、网络和合作组织的信任关系。
- 真实性（Authenticity）：是指保证网络系统中的实体（包括用户、进程、设备等）确实是其所声称的特性。
- 抗抵赖性（Non-repudiation）：是指保证网络实体不能否认其行为或操作的特性。

由上述定义及其在信息安全保障体系建设中的重要性可以看出，保密性、完整性、可用性和可靠性是信息安全保障中各类系统及其所承载信息的普遍性质。因此，本文把保密性、完整性、可用性和可靠性定义为信息保障的基本性质。真实性、抗抵赖性和可控性是对于某些系统信息保障中数据认证和通信抗抵赖等的特殊需求，因此定义为信息保障的特殊性质，如在电子商务系统中对抗抵赖性有较高的要求。这样划分既充分考虑了信息系统的安全保障需求，又能保证信息系统安全保障分级的科学性。表 6-1 展示了电子政务信息资源共享各阶段的保障目标。

表 6-1　电子政务信息资源共享各阶段的保障目标

	保密性	完整性	可用性	可信性	真实性	抗抵赖性
采集			√	√	√	
存储	√	√	√			
传输	√	√	√		√	√
交换	√	√	√	√	√	
处理	√	√	√			√

6.2.3　安全威胁维

复杂性科学承认个体与环境的相互影响和相互作用，它是系统演变和进化的主要动力。通过主体和环境间的相互作用，使得个体变化成为整个系统变化的基础，从而影响系统的宏观行为。电子政务的每个发展阶段都是与特定历史条件下信息化和信息安全的大环境相对应的。信息化程度越高，电子政务应用范围越广，信息安全问题就越突出。在当前时期，电子政务的安全环境非常复杂，社会环境的威胁、技术环境的脆弱和物理自然环境的恶化等都会给电子政务的安全保障带来众多隐患。

1．社会环境威胁

社会环境威胁主要是指敌对组织、恐怖势力或其他别有用心的团体及个人通过对电子政务环境中网络的破坏、信息的窃取及人员的利用，破坏我方利益，达到其不良政治或商业目的。

2．技术环境威胁

技术环境是指电子政务信息系统的技术因素，包括网络结构、软硬件设施、信息流、信息处理、信息传输、信息存储等多个方面。

3．物理自然环境威胁

物理自然环境包括物理基础支撑环境和自然环境的变化。由于电子政务系统对信息网络的高度依赖，自然环境威胁，如地震、雨雪、飓风、海啸等往往会给电子政务的生存环境造成毁灭性的打击。

安全威胁从宏观上来看是由安全环境所决定的，从微观上来看则源于各种攻击行为，每种攻击行为都可相应地破坏一种或多种安全属性。

1．信息泄露

指信息被泄露给某个未授权的实体。这种威胁主要来自如窃听、搭线或其他信息探测攻击等行为，主要破坏信息的保密性。

2．完整性破坏

指信息或信息系统通过未授权的创建、修改或破坏而受到损坏。这种威胁主要来自外部攻击或自然灾害，主要破坏信息或信息系统的完整性。

3．拒绝服务

指对信息资源的合法访问被无条件阻止。这种威胁主要来自攻击者的大量访问导致的负载或系统在物理上或逻辑上被中断，主要破坏信息系统的可用性。

4．非法使用

指某一信息资源被某个未授权的实体或以某一未授权的方式使用。这种威胁主要来自人为攻击，主要破坏信息或信息系统的可信性。

5．仿冒攻击

指某个非法实体假装成另一个合法实体渗入某个安全防线，攫取该合法实体的权限进行访问或发起攻击。这种威胁主要来自人为攻击，主要破坏信息系统的真实性。

6．非法控制

指攻击者为获取未授权的权限而对系统实施的攻击，如僵尸网络。这种威胁主要来自恶意程序或人为攻击，主要破坏信息系统的可控性。

6.2.4 保障措施维

本报告认为，战略保障、管理保障和技术保障是电子政务信息资源共享安全保障措施的三个基本要素（见图 6-2）。

信息安全具有很强的对抗性、渗透性和整体性，是事关国家安全和社会稳定的全局性问题。因此，电子政务信息资源共享的安全保障机制建设需要从战略层面进行整体规划和总体设计。

管理制度的建立是电子政务信息资源共享安全保障机制建设的关键环节。它涉及国家、地区、行业、单位和个人的各个层面的综合协调、协同配合。只有科学有效的管理机制才能把信息系统中人的因素和技术因素合理地组织起来。

技术基础设施是建设电子政务信息资源共享安全保障机制的重要工作。它涉及密码技术、安全协议、安全系统、安全芯片、电磁辐射防护、恶意代码检查过滤、安全漏洞分析、安全检测及评估、应急处理和恢复、犯罪取证与保持等众多方面。目前，我国信息安全技术能力仍然相对落后，许多方面处于受制于人的状态，大力开展信息安全基础理论、关键技术和适应国情的方法和手段的研究，是形成信息安全保障能力的关键。

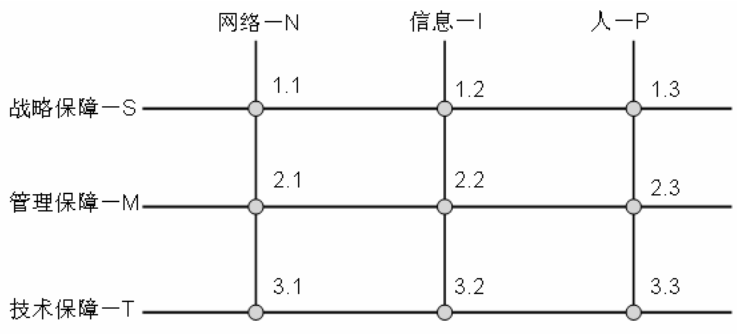


图 6-2　电子政务信息资源共享的安全保障机制（SMT-NIP 体系）

6.3　战略保障机制

战略无处不在、无时不在。从个人角度而言，一个人决定其所从事的职业即是一个长期战略。为实现这一目标，需要设定一些明确的目标和确定实现目标所需的努力。对于一个国家而言，政府制定经济、政治和社会等方面的发展战略，并通过法律、法规、政策和项目等方面来保证这些战略的实施。

一般而言，“战略”泛指在一定的历史时期内具有全局性、长期性、层次性、协调性和相对稳定性的谋划，它是由战略目标、战略重点、战略步骤组成的整体

性的系统决策方案。毛泽东指出，研究带全局性的战争指导规律，是战略学的任务；研究带局部性的战争指导规律，是战役学和战术学的任务。只要有战争，就有战争的全局。世界可以是战争的一全局，一国可以是战争的一全局，一个独立的游击区、一个大的独立的作战方面也可以是战争的一全局。凡是带有要照顾各方面和各阶段的性质的，都是战争的全局[129]。可见，一个国家、一个行业、一家企业的信息安全保障的整体性问题当属于战略学的研究任务。将电子政务信息资源共享的安全保障问题纳入战略层面加以研究，就是要对政务信息资源共享的安全保障机制建设的全局性、长远性和主导性问题加以研究分析，抓住研究问题的主要矛盾，为具体对策措施的研究提供思路和方向。

6.3.1 战略方针

按照战略学的研究思路，战略方针是一个战略的指导思想，是确定战略目标和战略对策的依据，是整个战略的灵魂。研究战略问题的首要任务是确定战略方针。

1．基本原则

从全局的角度审视电子政务信息资源共享的安全保障问题，首先需要处理好两对关系：一是要处理好信息公开、信息资源共享与信息安全的关系；二是要处理好深化应用与自主可控的关系。明确好这些问题是开展顶层设计和实施具体工程的基础，是在全国范围内进行基础设施建设的前提。

（1）处理好信息公开、信息资源共享与信息安全的关系

正确处理好信息公开和信息安全之间的关系，需要我们以辩证的眼光看待问题，既不能为了公开而忽视安全，也不能将安全问题绝对化，阻碍信息公开和应用发展。要围绕公众和企业最关心、最直接、最现实的利益问题，“以公开为原则，以不公开为例外”，编制政府信息公开目录，保证信息的准确性、完整性和时效性；通过制度建设，形成安全与应用相互促进的良性发展机制；提高政府的透明度和

[129] 毛泽东．中国革命战争的战略问题．毛泽东选集：第一卷[M]．北京：人民出版社，1991.

办事效率；保证人民群众依法行使选举权、知情权、参与权和监督权。

信息资源共享和业务协同给电子政务信息安全保障带来很大的挑战。当前，我国电子政务信息资源共享和业务协同能力不强问题突出，各部门丰富的信息资源还没有形成共享机制。其中一个重要的问题就是信息安全问题或对信息安全的信心难以得到保障。电子政务是一个多域（multi-domain）环境。电子政务架构的特点是不同类型政府机构间存在不同的安全策略，从而构成一个高度异构的多域环境。由于每一个机构的电子政务系统的安全目标不同，处理信息的敏感级别不同，面向的服务对象不同，因此，电子政务系统之间的跨域访问和信息交换与共享问题十分复杂。这不仅要依赖身份认证、访问控制等技术手段，更重要的是需要从战略层面规划设计出系统性的标准体系和政策法规。

（2）处理好深化应用与自主可控的关系

在全球化、信息化的环境中，高回报和高风险是成对出现的，在政府信息化纵深推进的同时，做到对电子政务网络、信息和内容的自主可控是涉及政府信息化工作可持续发展和国家安全与稳定的关键。随着信息技术的广泛应用，视频、语音、文本等数据的信息传输手段逐步融入电子政务应用之中，电子政务的潜在安全问题越来越多，安全技术和应对难度越来越大。因此，自主可控的战略目标要始终贯穿电子政务建设的各个环节，稍有不慎，就会给将来系统信息安全保障带来更多的复杂性问题和安全隐患。

近年来，我国电子政务基础设施建设取得了长足的发展，但是与建成自主可控的电子政务信息安全体系的目标仍存在一定的差距。利用当前信息基础设施更新换代和信息通信新技术迅猛发展的难得机遇，把掌握信息产业核心技术的自主知识产权作为提高我国产业竞争力和推动经济发展方式转变的突破口，创造良好的创新环境，对提高我国电子政务系统的自主可控能力、完善国家电子政务信息安全保障体系建设具有重要的现实意义。

2．战略方针

针对电子政务信息资源共享安全保障机制建设，本文提出二十四字方针，即“以服务为导向，以效益为中心，以安全保共享，以共享促安全”。

以服务为导向，就是要按照建设服务型政府的要求，以政府信息资源的公开、共享不断扩大公共服务范围，逐步形成惠及全民、公平公正、可持续发展的公共服务体系，切实提高为经济社会发展服务、为公众服务的能力和水平。

以效益为中心，就是要讲求实效，坚持经济效益和社会效益相统一，加强已有网络和信息资源的整合，避免重复建设，促进互联互通。

以安全保共享，就是要不断完善电子政务网络与信息安全保障体系，提高网络与信息安全保障能力，化解信息资源共享过程中产生的各种风险和威胁，为信息资源共享创造一个良好的安全环境。

以共享促安全，就是按照“积极防御、综合防范”的要求，不是被动地就安全抓安全，而是在发展中求安全。

6.3.2 战略重点

1．以政务信息资源开发利用为主线

《国家电子政务总体框架》（国信〔2006〕2 号）明确提出，要以政务信息资源开发利用为主线，建立信息资源共享和业务协同机制，更好地促进行政管理体系改革，带动信息化发展。可见，做好信息资源建设是推动信息资源共享和业务协同工作的基础和关键。长期以来，各职能部门条块分割的现状，严重影响着政府部门之间的信息资源共享和业务协同。因此，做好政务信息资源的规划和整合，统一信息资源建设，是信息资源开发利用的关键工作。其中一个重要措施就是要借助云计算和虚拟化等新技术，分阶段、分层次地部署国家电子政务信息资源管理中心建设。

2．以政务网络的建设为突破

统筹推进国家电子政务信息资源共享的网络设施建设，改善政务网络结构不合理和互联互通不畅等问题，重点发展面向公众服务的电子政务。明确政务内网、政务外网和基于互联网的政务应用的功能和定位，大幅提高政务网络的社会管理和公共服务职能。提高网络的互联互通程度，加强网络信任体系建设，有效保障

信息资源共享和业务协同的实施。在基层政府，要推行以互联网为基础的电子政务，大力提升政务信息资源的服务范围。充分将云计算、物联网和社交网络等新技术、新手段、新应用融入政务网络，提高政府对外宣传、汇集民智、体现民意和服务民生的能力。

3．以推进信息安全体系建设为保证

电子政务信息安全体建设就是按照中办发〔2002〕17 号文件、中办发〔2003〕27 号文件、国信〔2006〕2 号文件等重要文件的要求，创建安全健康的网络环境，保障和促进政府信息化的健康发展，保护公众利益，维护国家安全。要坚持“积极防御，综合防范”的总方针，完善组织管理体系，落实信息安全管理责任制；加强以密码技术为基础的网络信任体系建设，完善信息安全监控体系，重视信息安全应急处理工作；加强信息安全技术研究开发，推进信息安全产业发展；加强信息安全法制建设和标准化工作；加快信息安全人才培养，增强用户信息安全意识；保证信息安全资金，全面提升政务网络的安全防护能力、隐患发现能力、应急处置能力和信息对抗能力。

6.4　管理保障机制

6.4.1　领导体制

领导体制是指为了实现领导意图和领导职能的机构设置及管理权限划分的制度，它涉及组织层次与管理幅度、领导机构内部各部门之间的职责与权限的划分，以及领导机构外部的职权关系等内容[130]。领导体制对于电子政务信息资源共享及其安全保障的效率具有根本性影响。事实上，电子政务共享过程中的许多问题，包括动力不足、发展不均、责权不明等，都与领导体制缺失有关。只有科学有效的领导体制才能把信息系统中人的因素和技术因素合理地组织起来。在电子政务

[130] 李平．政府领导体制与行政效率研究[J]．政治学研究，2001（1）：56．

信息资源共享安全保障工作上，需要一个顶层、专管、超脱、强力的领导和协调机构。它涉及国家、地区、行业、单位和个人的各个层面的综合协调与协同配合，如图 6-3 所示。

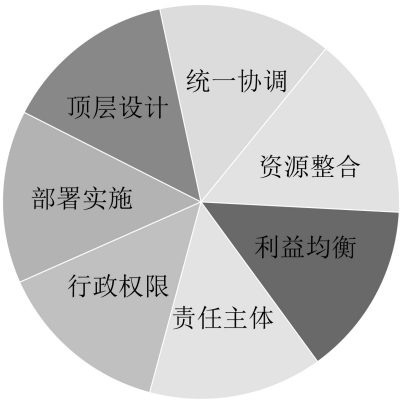


图 6-3　电子政务领导体制承担的职责

6.4.2　法律保障

电子政务相关立法是电子政务信息资源安全共享的前提，通过相关法律法规的制定，在法律上明确权责关系。电子政务信息资源共享安全的法律保障主要分为立法、执法、普法三个环节的保障，如图 6-4 所示。

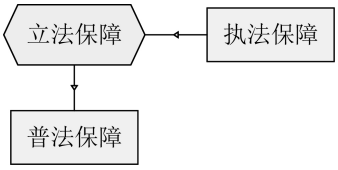


图 6-4　电子政务信息资源安全共享的法律保障

1．立法保障

根据目前电子政务信息安全保障的现状和问题，将立法保障分为基本法、专门法、相关法和政策体系。

基本法是一部具有宏观指引意义的法律规范，需要明确电子政务信息资源共享安全保障的立法宗旨、指导思想、基本原则、保障对象等基础性问题，为总体框架的设计打下坚实的基础。基本法不能将涉及信息安全保障的内容融入相关法律的过程中，应避免规范之间内容冲突、重叠等问题。

专门法是电子政务信息资源共享和信息安全的法律与规章，包括规范行为主体的法律，如保密法、隐私法；规范主体行为的法律，如电子签名法；规范流程的法律，如信息安全保护条例、软件保护条例等；规范资格的法律，如国际联网管理规定。

相关法规和条例，如政府信息公开条例、互联网信息管理办法。

政策体系（国家宏观政策、战略规划中关于法律体系建设的部分，以及全国人大的决定，中办、国办的通知等），如《全国人民代表大会常务委员会关于维护互联网安全的决定》、《关于政府上网信息保密管理的通知》。

法律修订也是立法保障的重要工作。若原有法律不适用，则会造成信息资源共享得不到保障。因此，通过对相关法律法规的修改、合并和补充，能够适时满足电子政务信息资源共享及其安全保障的需要。

2．执法保障

电子政务信息资源共享安全的执法保障涉及执法机构、执法人员和司法保障三个方面，要健全电子政务信息安全执法机制，建立专门的信息安全执法机构，提高信息安全执法人员的素质。

另外，从广义上来说，执法保障包括行政执法和司法保障。对于电子政务信息安全保障来说，主要是法院、检察院等司法机关对信息安全违法案件进行侦查、诉讼等保障手段。

3．普法保障

一是法律法规宣贯。宣贯是有针对性地开展信息安全法律法规的指导培训工作，明确各方职责，提高电子政务信息资源共享的效率和整体安全保障水平。

二是建立信息安全文化。这也是普法的一个方面，需要每一个参与者都是保

证电子政务安全的重要执行者，利用各种宣传和培训手段，在全民中普及信息安全意识。

6.4.3 管理制度

根据电子政务信息资源安全共享的内容、环节、要求等，要建立包括保密制度、灾备制度、检查评估制度、监控预警制度、应急响应制度、监督管理制度等在内的制度体系，充分保障共享的整体安全，如图 6-5 所示。

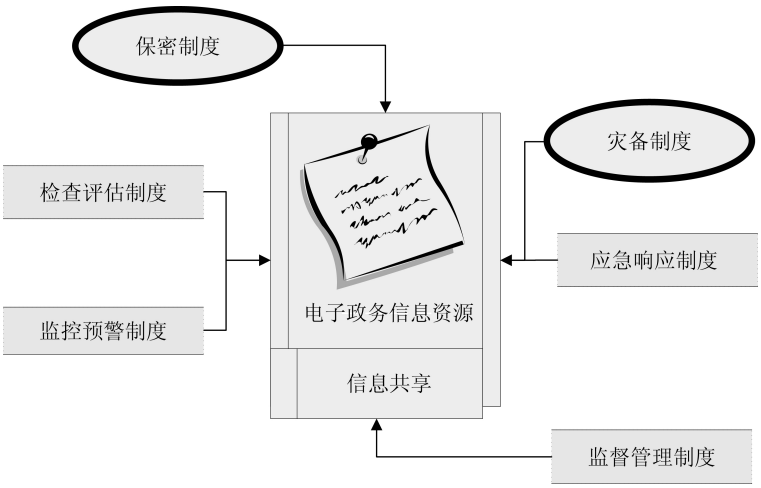


图 6-5　电子政务信息资源安全共享的制度保障

1．保密制度

2010 年 4 月 29 日修订通过的《中华人民共和国保守国家秘密法》对保密制度做出了明确细致的规定，具体到涉密部门、涉密人员及其行为规范。“涉及国家安全和利益的事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为国家秘密。”[131]电子政务信息资源中敏感类型复杂多样，

[131] 中华人民共和国主席令第二十八号《中华人民共和国保守国家秘密法》第十条，2010 年 10 月 1 日起实施。

从政府信息资源共享的角度分析，综合考虑保密级别、需求程度和共享服务能力等因素，可将政务信息资源划分为：

- 强制共享类，即可供相关政府职能部门或履行公共管理职能的组织无条件共享利用的政务信息资源。
- 条件共享类，即只能按有关规定提供给指定单位共享利用的政务信息资源。
- 不予共享类，即不能提供给其他职能部门及其他履行公共管理职能的组织共享利用的政府信息资源。

对于不予共享类信息，应列为保密信息，进行严格的保密管理。政府信息资源保密管理制度要依据国家安全保密标准、文件和要求进行编制，覆盖电子政务信息资源共享的各个涉密环节，形成科学有效的制度体系结构。

通常信息安全保密制度可分为三个层面：基本制度、二级制度和专项制度[132]。基本制度是指日常保密管理工作规范；二级制度是根据工作实际制定的细化、具体的保密管理措施；专项制度是针对重大涉密项目制定的专门保密管理措施。电子政务信息资源保密管理制度采用统一管理、分层制定的模式，能够将保密要求转化为具体的操作重点，以便更好地降低泄密风险，保护国家重要信息资源。

2．检查评估制度

检查评估制度要求通过风险评估等手段来实现电子政务系统的攻击检测和漏洞检测，掌控信息系统存在的弱点和漏洞，以及面临的威胁和破坏，通过控制风险、降低风险和转移风险来保障电子政务信息系统安全。信息安全风险评估是电子政务信息安全保障体系工作的重要内容，是对电子政务系统实施安全管理的有效手段。

3．监控预警制度

监控和预警的目的是防患于未然，即在安全事件来临之前或还未造成严重后

[132] 张朝等．军工行业信息安全保密管理制度规范化探讨[J]．保密科学技术，2011（4）：37.

果之前，能及时发出预警信息，制止事态的进一步发展。需要各级基础信息网络和重要信息系统的主管部门和运营企业从制度建立、技术实现、业务管理等方面建立健全通信网络安全的预防和预警机制。

（1）预防机制

各级电子政务主管部门加强对网络安全防护工作和应急处置准备工作的监督检查，保障通信网络的安全畅通。

（2）预警监测

各级电子政务网络主管部门和管理机构及运营企业建立相应的预警监测机制，加强通信网络保障预警信息的监测收集工作；各级电子政务网络主管部门与国家、地方政府有关部门建立有效的信息沟通渠道；各级基础网络运行管理维护部门对网络日常运行状况实时监测分析，及时发现预警信息。

（3）预防预警行动

国家电子政务网络安全主管部门获得预警信息后，通信保障应急领导小组立即召开会议，研究部署网络保障应急工作的应对措施，通知相关运营企业做好预防和通信保障应急工作的各项准备工作；各级电子政务网络安全管理部门通过监测获得内部预警信息后，对预警信息加以分析，按照早发现、早报告、早处置的原则，将可能演变为严重通信事故的情况，及时报告给国家相关机构。

（4）预警信息通告

预警信息是指存在潜在安全威胁或隐患但尚未造成实际危害和影响的信息，或者对事件信息分析后得出的预防性信息。预警信息分为 I 级、II 级、III 级、IV 级，I 级为最高级。预警信息通告内容主要包括：受影响的系统、可能产生的危害和危害程度、可能影响的用户及范围、建议应采取的应对措施及建议[133]。国家通信保障应急领导小组可以确认并发布 I 级预警信息；省（区、市）通信管理局通

[133] 关于印发《互联网网络安全信息通报实施办法》的通知（工信部保〔2009〕156 号）[EB/OL]. 2009-04-13.

信保障应急管理机构可以确认并发布 II 级、III 级和 IV 级预警信息[134]。预警过程描述如表 6-2 所示。

表 6-2　预警过程描述

预警过程	要　　求
预警监测	是否按要求实施定期的漏洞检测
预警信息管理	定期发布、更新预警信息
按预警等级由规定单位发布预警信息	按国家或行业相关文件执行
预警准确性	成功预警次数比总预警次数

4．灾备制度

灾难备份是为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、技术支持能力和运行管理能力进行备份的过程[135]。灾难备份是确保电子政务系统在社会紧急状态下仍能保证其主要业务健康运行的有效手段。电子政务信息资源是灾难备份建设的重中之重，要求配备能够在灾难发生时接替数据处理和系统运行的各种资源。

灾难恢复是信息安全保障工作的重要环节，是指系统在遭受攻击和破坏后，应能启动应急预案，并具有与之配套的诸如灾难备份、容错、冗余、替换、修复等技术和管理手段，保证系统能在最短的时间内得到恢复，保障主要业务的正常运行。电子政务系统灾难恢复工作要求充分考虑电子政务系统的抗毁性和灾难恢复，制定和不断完善信息安全应急处置预案。

灾难恢复技术是业务连续性技术的基础，它能够为重要信息系统提供发生灾难时保持持续运行的能力。灾难恢复措施包括灾难预防、容灾演练和实际灾难恢复。

① 灾难预防。为预防灾难的发生，需要进行容灾备份。

② 容灾演练。为保证灾难恢复的可靠性，需要进行定期的容灾演练，以熟练灾难恢复的操作过程，提高人员的安全意识和灾难恢复能力，并检验灾难恢复流程是否存在缺陷。

[134] 国家通信保障应急预案[EB/OL].[2011-10-15].www.gov.cn/yjgl/2006-01/24/content_170422.htm.
[135] 国务院信息化工作办公室．重要信息系统灾难恢复指南[S]．2005：4.

③ 实际灾难恢复。在出现突发的信息安全事件时，应立即执行灾难恢复计划，按照预先制定的人员安排、工作流程、资源部署方案，对信息系统进行灾难恢复工作，保证其在最短时间内恢复正常的功能。

5．应急响应制度

应急响应是对危及电子政务信息资源共享安全的事件、行为、过程做出及时、准确的响应处理，综合利用检测、抑止、根除、恢复等手段，杜绝危害的进一步扩大，保证电子政务系统能够正常提供服务。应急响应的目标是将电子政务系统的主要功能遭到的任何破坏或攻击控制在频率低、跨时短、地域上可隔离、对国家和组织造成的损失降低到最小的程度，使信息系统在面临攻击的情况下仍能够有效运行，尽可能地减少攻击造成的损失。

可从不同规模安全事件的反应时间、技术手段、管理措施、处理效果等方面进行考评，该过程通过建立应急响应体系来实现。一个完整的应急响应体系由三部分内容构成：应急组织体系、应急服务体系和应急技术体系，如表 6-3 所示。

表 6-3　信息安全应急响应体系

组织体系	服务体系	技术体系
1．建立应急响应小组 2．制定严格的安全保密制度 3．具有良好的合作机制	4．技术储备 5．预警和报警 6．事件处理 7．脆弱性处理 8．安全审计和评估 9．安全攻击的配置和维护	10．建立预案库 11．威胁抑止 12．追踪 13．知识汇总 14．交流与协作

应急响应工作不仅是单纯的技术问题，还涉及政策、法规、标准等诸多因素。突发事件发生时，按照分级负责、快速反应的原则，将通信保障和通信恢复应急响应工作划分为 4 个等级：I 级、II 级、III 级和 IV 级。

6．监督管理制度

建立第三方监督机制。确定技术问题由中立的、具有公信力的、且经政府主管部门认可的技术检测机构来进行检测，作为行政执法部门评判的依据。

在具体的信息安全监管过程中，行业组织、技术联盟、私营部门等具有极强的影响力，它们通过制定行业规则、技术标准等手段，加强对信息安全的监管。在完善政府主导的治理模式的同时，邀请自律性监管主体参与其中，分明职权，共同监管。

6.4.4　标准体系

一般来说，信息资源标准可分为信息技术标准和信息管理标准。对于电子政务信息资源共享的安全保障来说，技术类标准主要包括信息资源共享的技术标准和信息安全技术标准，完整的信息技术标准体系应贯穿从信息采集到信息使用的全过程；管理类标准主要涉及政府信息的有效使用和安全管理，如信息使用流程管理、信息资源评价、信息服务、信息安全管理标准等，如图 6-6 所示。

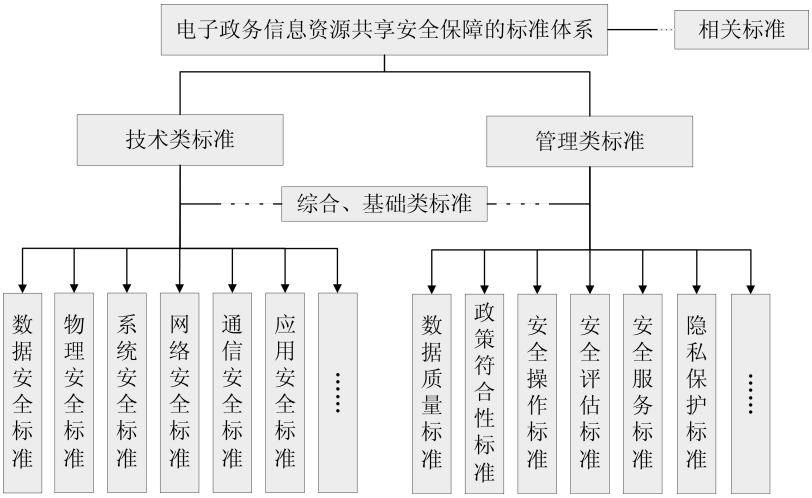


图 6-6　电子政务信息资源共享安全保障标准体系构建

1．技术类标准

数据安全标准：保护电子政务信息资源共享中的数据安全，确保经过电子政务网络传输和交换的数据不会发生增加、修改、丢失和泄露等。

物理安全标准：保护电子政务系统的硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击，防止通过内部环境与外界敌对环境之间的物理联系而使电子政务信息资源共享遭受网络侵袭。

系统安全标准：保障电子政务系统的可用性、可控性等安全属性的技术性标准。

网络安全标准：有效避免黑客攻击、计算机病毒、拒绝服务攻击等网络威胁，保护电子政务信息资源共享避免遭受网络中断、窃听、信息篡改、身份假冒等网络安全问题。

通信安全标准：防止通信网络阻塞、中断、瘫痪或者被非法控制，防止通信网络中传输、存储、处理的数据信息丢失、泄露或者被篡改。

应用安全标准：保障电子政务信息资源共享的应用系统和应用程序使用过程和结果的安全，消除计算、传输数据的泄露和失窃等隐患。

2．管理类标准

数据质量标准：解决电子政务信息资源采集和共享过程中的采集误差，保障信息的准确性和一致性，提高共享效益和质量。

政策符合性标准：保证电子政务信息资源共享符合国家有关政策法规的要求，包括信息公开和信息保密等要求。

安全操作标准：规范电子政务系统的操作者必须养成一些良好的安全习惯，以免成为黑客或恶意分子的利用对象。

安全评估标准：对信息安全产品或系统进行安全水平测定和评估的一类标准，包括评估方法、评估模型、评估流程等。

安全服务标准：对电子政务信息安全服务的组织、设备、质量等提出的规范性要求。

隐私保护标准：规范电子政务信息资源共享中对个人隐私的保护，提出保护公民个人信息的准则。

管理创新包括将一种新关系、新体制或者新机制引入人类社会的经济活动中，并推动社会和经济发展。可以把制度解释为一种体制和机制，体制是指的机构，机制是指的程序和过程。

6.4.5　信任机制

1．信任的概念

信任是一个非常复杂的社会与心理现象，信任仅作为一种微观的社会关系是不完全充分的，需要借助其他社会力量共同实现[136]。信任是基于制度的，是在特定的法律制度、社会规范基础上形成的，制度保障能够降低感知的风险[137]，使人感到环境的安全性。信任有三个层面：一是基于交往经验的信任，这种信任来自互动、交换和交易经验的积累，互惠是核心；二是基于行动者具有社会、文化共性的信任，它根源于社会模仿的义务和合作规则；三是基于制度的信任，这种信任是建立在非个人的规则、社会规范和制度基础上的。

2．信任机制构建

电子政务信息资源共享的信任机制通过三个方面来构建：一是技术规范，是实现共享与协作的基础，可以使电子政务业务的各参与方从技术层面保证信息资源共享的安全性，并搭建可以实现信息资源共享的电子政务平台；二是制度支撑，是实现共享与协作的关键，要求其保证有共享需求的单位可以从相应的渠道获取相关共享信息；三是建立合作，共赢的合作关系是实现共享与协作的动力。

（1）技术规范

网络信任体系是信息安全保障体系建设的重要组成部分，它以密码为基础，以法律法规、技术标准和基础设施为主要内容，以解决网络应用中的身份认证、

[136] 卢曼．信任：一个社会复杂性的简化机制[M]．上海：上海人民出版社，2005．

[137] Zuker, L.G. Production of trust: institutional sources of economic structure[M]. Greenwich, CT:JAI Press, 1986.

授权管理和责任认定为目的[138]。由于电子政务活动包含两方面的内容，一是面向社会公众的活动，二是面向政府机关内部的活动，二者服务对象不同，活动性质也不同，其电子认证问题也具有不同的特殊性，因此不能完全由社会第三方提供服务。网络信任体系的技术细节详见 6.5 节。

（2）制度支撑

① 信息资源公共服务机制。

从共享模式来看，电子政务信息资源共享分为纵向部门间 G2G 共享和横向 G2G 共享。传统职能型组织的管理模式（见图 6-7）已不适应新时期政府管理和政府信息资源共享的需求，而网络型组织（见图 6-8）可为政府管理和政府信息资源共享提供有效的模式和建设基础，是当今的发展趋势。电子政务信息资源共享要求提高提供部门间信息资源共享服务的能力，有效整合并利用现有资源，实现部门间的互联互通和政务信息的共享。

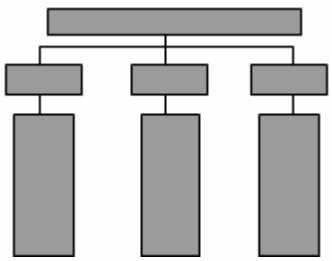


图 6-7　传统职能型组织模式

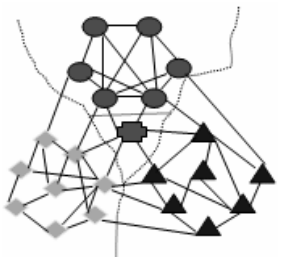


图 6-8　网络型组织

② 对标准规范的执行力度。

统一标准是实现部门间互联互通、信息资源共享和业务协同的基础。电子政务标准必须充分发挥对电子政务信息资源共享和电子政务安全保障建设的导向作用和协调优化功能，以确保电子政务整体效能的实现和系统的安全可靠性。

[138] 国务院办公厅转发国家网络与信息安全协调小组《关于网络信任体系建设的若干意见》（国办发〔2006〕11 号文件）. 2006-02-23.

（3）合作共赢

共享过程中会触及组织的利益，并带来相应的风险。通过风险界定可以规避可能和潜在的风险。例如，组织 A 和组织 B 在一次联合活动中需要合作，如果组织 A 向 B 共享了一条信息，而这条信息对整个活动的成功非常有利，但 B 向 A 隐藏了一条非常重要的信息，在整个活动中 B 的表现就会好于 A，因而具备了竞争优势。这在博弈论中是一个典型的囚徒困境（见图 6-9）的样例。

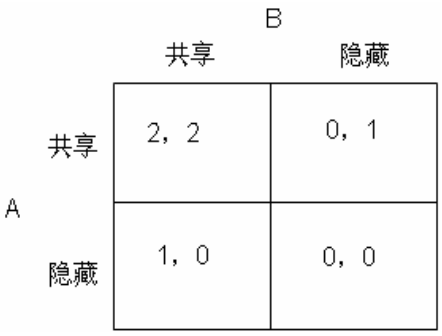


图 6-9　政务信息资源共享中的囚徒困境

在纵向较为封闭的行政体系中，竞争在一定程度上占据上风，从而致使双方都会想方设法地隐藏信息，进而陷入“隐藏－隐藏”的困境。在信息化社会，封闭式的纵向行政关系发生了变化，组织机构间逐步变成网络型的关系，组织间的有效协作和信息的及时交互在处理应急事件中的作用愈发明显。在建设服务型政府理念的驱动下，“共享－共享”模式的共赢作用逐渐突出，政府机构间的共享效益和积极性相应提高，有利于实现政府协同办公和信息资源共享的良好局面。

6.4.6　人才保障机制

1．人才配置

人才资源是电子政务信息资源共享安全保障中具有决定意义的资源。人才资源的合理配置，对电子政务信息安全保障至关重要。

电子政务信息资源共享安全保障的人才需求结构如表 6-4 所示。

表 6-4　信息安全人才体系构成

人才类别	人才指向
复合型管理人才	各级政府中指导和规划信息安全保障工作的人才、各行各业的信息安全管理人才
创新型研发人才	熟悉信息技术、信息安全技术并对安全问题有深入研究的专家
网络安全管理人员	分布在政府、企事业单位网络系统的安全管理员
信息安全应用人才	政府、基础信息网络、重要信息系统、企事业单位信息系统的使用者
普通民众	使用互联网和其他 ICT 产品（如移动通信设备）的普通公民

各类人才需要具备的素质如下：

① 复合型管理人才需要具备政策、经济、信息安全、公共管理等各个方面的知识和能力，具有战略的眼光、技术的背景和管理经验，综合性强。

② 创新型研发人才作为构建创新型国家和建立具有自主知识产权的信息安全产业的中坚力量，要求精通技术、有一定研究能力、创新能力强。

③ 网络安全管理人员需要具备较高的素质和责任心，对他们进行经常性的高质量培训也很重要。

④ 信息安全应用人才需要具备较强的信息安全意识，要落实安全责任制，做好本系统的信息安全工作。

⑤ 普通民众需要掌握最基本的信息安全防护措施和技能，接受信息安全普及教育，协助做好家庭等小型用户的信息安全保障工作。

2．人才培养

电子政务信息资源共享的安全保障人才培养要从层次结构和比例结构两个维度来考虑。在层次结构上，分为研究生、本科生、专科生（含高职、中专、职高生）三个层次，其人数比例即为比例结构。

在培养层次上，以本科教育为依托，重点抓好高层次的研究生培养和面向基层部门的大中专生培养；人才培养的比例结合实际社会需求来拟定。

在培养模式上，高校培养以应用型人才为主体，与基层部门合作，开展多种形式联合办学；开展岗位培训，以及发展在职和继续教育的培养方式，切实提高电子政务在职人员的信息安全素养；利用广播、电视、计算机网络等对偏远地区开展各种信息安全远程教学。

6.5　技术保障机制

对于电子政务信息系统来说，围绕保障对象要素——网络、信息和人来设计建立安全保障策略是保障政务信息资源安全共享的可行方法。归纳起来，就是要做好电子政务网络安全域划分、敏感信息分类和人员身份管理（见图 6-10）。

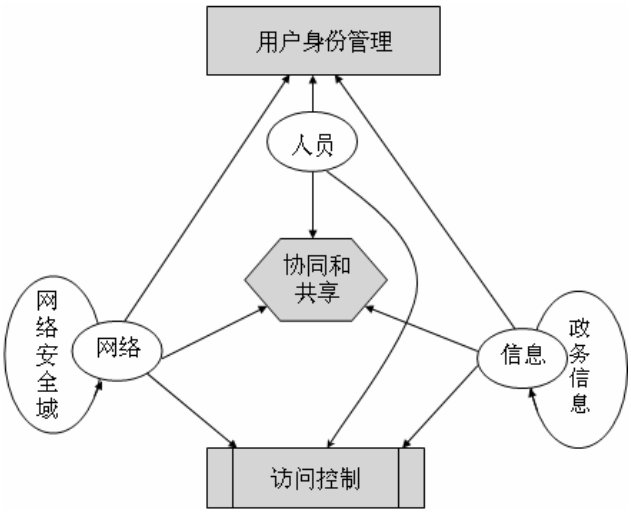


图 6-10　电子政务信任体系建设

6.5.1　网络分域

安全域是指由实施共同或相似安全策略的主体和客体组成的集合。安全域的划分主要遵从以下原则：系统功能和应用相似；信息资产价值相似；安全需求相

似；环境威胁相似。安全域既可以从物理上划分，也可以从逻辑上划分。安全域的物理划分依据网络系统所处的物理位置，如地理位置、建筑大楼等。安全域的逻辑划分则依据国家政策和管理规范，如政府专网、政府外网等。从逻辑上划分的安全域，更易于反映出安全政策的要求。不同信息安全域之间的信息交互主要通过访问控制、鉴别服务、数据完整性检测、数据保密和抗抵赖性等技术措施来实现，以保证信息在交换和共享过程中的保密性、完整性和可用性。

从安全域的定义来看，一个网络系统本身就是一个安全域，而组成系统的一个子系统也可以构成一个安全域，在实践中则需要根据实际需求来确定安全域的精细程度，从而实施具体的划分。

1．国家电子政务网络安全域的经典划分

根据中办发〔2002〕17 号文件《国家信息化领导小组关于我国电子政务建设指导意见》和中办发〔2006〕2 号文件《国家信息化领导小组关于推进国家电子政务网络建设的意见》的精神，统一的国家电子政务网络由基于国家电子政务传输网的政务内网和政务外网组成。

（1）政务内网

政务内网由党委、人大、政府、政协、法院、检察院的业务网络互联互通形成，主要满足各级政务部门内部办公、管理、协调、监督及决策的需要。政务外网主要满足各级政务部门进行社会管理、公共服务等面向社会服务的需要。充分利用国家公共通信资源，形成连接中央和地方的统一的国家电子政务传输骨干网。中办发〔2002〕17 号文件将电子政务内网定义为含有国家涉密内容的网络信息系统。涉及国家秘密的电子政务内网与国家安全密切相关，内网一旦“失守”，将直接危害到国家利益。

（2）政务外网

依据上述要求，国家电子政务外网（简称政务外网）的总体目标是依托统一的国家电子政务外网，建立覆盖全国各级政务部门面向社会管理、公共服务的网络基础设施、信息资源体系、服务与应用体系、法律法规与标准化体系、管理体系，支持电子政务业务系统的运行，支持跨部门、跨地区的信息资源共享，支持

电子政务业务系统的互联互通和信息交换，促进各级政务部门政务监管能力和服务水平的提升。

（3）基于互联网的公共服务网

互联网是我国重要的信息基础设施和战略资源，积极利用互联网进行电子政务建设，既能节约资源、降低成本，又能提高效率、扩大服务的覆盖面。因此，基于互联网进行电子政务建设，对于发展中国家来说，具有重要的战略意义和现实意义。基于互联网的电子政务（E-Government based on Internet）是指依托互联网，将对内的政务办公、对外的公共服务和政府间的信息资源共享集成在同一个网络平台下的电子政务应用。原国务院信息化工作办公室于 2005 年 10 月在河南省济源市开展了基于互联网的电子政务信息安全保障试点工作，将“内部网络”和“外部网络”完全建构在互联网上，同时综合运用以密码技术为基础的信息安全技术，兼顾开放和安全，建成了低成本、可扩展的电子政务网络，仅一次性投资就节省了近千万元。因此，业界也将基于互联网的电子政务称为电子政务建设的“济源模式”。同时，利用互联网开展电子政务建设面临着比内、外网更大的外部威胁，如计算机病毒传播和扩散、恶意网络攻击、身份假冒、信息泄露等信息安全威胁和风险。在进行基于互联网的电子政务安全保障体系设计中，可根据系统使命和安全需求将其划分为多个不同的安全域，主要包括：

① 内部数据处理区域，指仅向政务办公人员开放的政务办公系统及其数据所在的区域。

② 公开数据处理区域，指面向公众开放的公共服务系统及其数据所在的区域。

③ 安全服务区域，指仅向系统安全管理人员开放的安全管理系统及其数据所在的区域。

④ 安全管理区域，指为用户提供安全服务的系统及其数据所在的区域。

在基于互联网的电子政务信息保护方面要实行分类防护办法，将信息分为公开、内部共享和内部受控等类别，根据信息类别提供不同的安全措施。对不同安

全域制定不同的安全策略，实施对各域信息的安全保护，以及提供对不同域间信息交换机制的安全控制。

2．基于“安全保护等级”的划分

信息安全等级保护是国家在国民经济和社会信息化发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化健康发展的基本制度（公通字〔2004〕66 号，以下简称“66 号文件”）。66 号文件中规定信息系统的安全等级从低到高依次包括自主保护级、指导保护级、监督保护级、强制保护级、专控保护级 5 个安全等级。2007 年 6 月，公安部、国家保密局、国家密码管理局、原国务院信息化工作办公室联合印发了《信息安全等级保护管理办法》（公通字〔2007〕43 号）。文件规定，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益及公民、法人和其他组织的合法权益的危害程度等因素确定；根据信息系统受到破坏后，对社会秩序、公共利益、国家安全造成影响的程度进行划分。等级保护工作从对基础信息网络和重要信息系统实施监管的角度出发，对促进电子政务信息安全保障工作有着重要的推进作用。但由于电子政务信息系统复杂多样，两个处于同一安全等级的信息系统，其保密性、完整性、可用性等安全需求和目标可能存在较大的差别。因此，安全等级还不能直接作为应用在两个信息系统间进行信息资源共享和交换、建立安全策略的依据，需要从更精细的角度进行研究分析。

3．基于安全保障目标使命和需求的划分

（1）确定信息系统的安全保障需求

面对复杂的电子政务网络信息系统，全面、准确地分析其安全保障需求是进行安全域划分和实施信息安全保障体系建设的基础。建议通过以下步骤分析电子政务系统的安全需求（见图 6-11）。

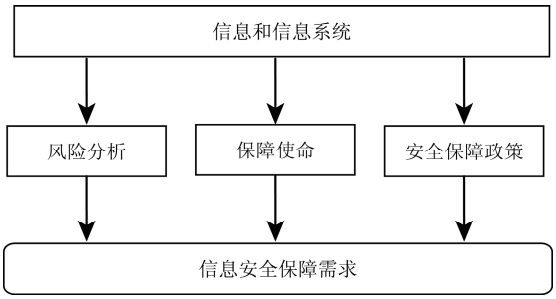


图 6-11　政务信息系统安全保障需求分析

① 界定研究对象，明确本系统信息安全保障的使命、目标和功能，分析系统在国家安全、社会稳定和经济发展中的地位和作用。

② 给出系统业务描述，包括本系统主要业务应用、业务流程和信息流程。

③ 针对本系统信息安全保障体系建设的使命、信息的重要程度、信息系统承载业务的重要程度、风险分析的结果、系统遭到攻击破坏后造成的危害程度等因素，确定本信息系统的安全保障总体需求。

④ 进一步明确系统对信息和信息系统的保密性、完整性、可用性、真实性、抗抵赖性和可靠性等安全保障属性的需求程度。

电子政务信息包括用户信息和系统信息。系统信息（如网络路由表、密码文件及密钥管理信息等）的保护必须与处理、存储和传输过程中最重要、最敏感的用户信息的保护目标相一致。信息的安全保障需求分为很高、高、中、低和很低 5 类，分别对应信息的某个安全属性的丧失对信息保障使命的影响的 5 个不同类别。

电子政务信息系统是指由软件、硬件、操作人员及系统所承载的信息构成的，按照一定的应用目标和规则实现对信息的采集、加工、存储、传输、检索等功能的人机系统。信息系统的安全保障类别依据系统信息，系统中处理、存储和传输的信息的保障类别来确定。信息的保障需求可形式化表示如下：

信息或服务 M 的安全保障需求 $S(M)=\{(C,X);(I,X);(A,X);(AT,X);(NR,X)\}$，其中 C、I、A、AT、NR 分别代表保密性、完整性、可用性、真实性和抗抵赖性，X=1,2,3,4,5

表述影响等级分别为很低、低、中等、高、很高。

例如，某系统所承载的信息 Z 的安全需求为{(保密性,很高)；(完整性,高)；(可用性,高)；(真实性,高)；(抗抵赖性,中等)}，可记为

$$S(Z)=\{(C,5);(I;4);(A,4);(AT,4);(NR;3)\} \tag{6-1}$$

（2）确定信息系统的安全保障级别

电子政务信息系统安全保障级别的确定应遵循以下原则。

① 信息保障的基本性质——保密性、完整性、可用性、可靠性等保障需求是确定信息系统安全保障等级的基础。真实性和抗抵赖性作为信息保障的性质，在制定信息保障策略时使用。

② 信息系统对保密性、完整性、可用性的保障需求取决于系统承载信息（或服务）的最高保障等级，即

$$X(C)=\max\{i(C_i,X_i)\,|\,1\leqslant i\leqslant M,i\in N\} \tag{6-2}$$

其中，$\max(\cdot)$ 表示对信息系统所承载（多类）信息（或服务）的某个安全属性的最高安全保障需求，$X(C)$表示信息系统的保密性等级，N 表示自然数。如信息系统 A 上承载着两类敏感信息（或服务）I_1 和 I_2，I_1 和 I_2 安全属性保障需求分别为

$$S(I_1)=\{(C,2);(I,3);(A;3)\} \tag{6-3}$$

$$S(I_2)=\{(C,4);(I,2);(A;3)\} \tag{6-4}$$

则系统 A 对保密性、完整性、可用性的安全保障需求为

$$S(A)=\{(C,4);(I,3);(A;3)\} \tag{6-5}$$

③ 取高原则。信息系统安全保障等级定义为对保密性、完整性、可用性和可靠性安全保障需求的最高级，即信息系统的安全保障等级

$$Y=\max\{X(C),X(I),X(A),X(R)\} \tag{6-6}$$

设 $X(R)=3$，根据取高原则，上述系统 A 的安全保障级别定义为 4。

（3）确定基础保障基线

“基线”对应的英文单词是 Baseline，其含义是一种用于测量或在测量中用于比较的标准。“基线”的概念已经应用于信息安全标准或规范当中，如美国 FIPS199 标准。本章把信息安全保障基线定义为实现其安全保障使命和功能的基本安全需求。根据安全保障等级划分方法，处于同一等级的系统在保密性和可用性方面可能会面临不同的保障需求，会对应不同的保障基线。因此，本章把保障基线分为基础（共性）保障基线（记为 FBL）和增强（特殊）保障基线（记为 ABL）。基础保障基线在某种程度上反映了政务信息系统的重要程度，它要求处于该级别的系统都需要具备基本的保障需求；增强保障基线则反映出政务系统的个体安全保障需求。保障基线的识别可以通过制定相关的国家标准来实施（见表 6-5）。

表 6-5　基于战略、管理和技术的基础保障基线

保障等级	技术（T）	管理（M）	战略（S）	FBL
第一级（很低）	T_1	M_1	S_1	IA_1
第二级（低）	T_2	M_2	S_2	IA_2
第三级（中）	T_3	M_3	S_3	IA_3
第四级（高）	T_4	M_4	S_4	IA_4
第五级（很高）	T_5	M_5	S_5	IA_5

（4）确定增强保障基线

基于信息保障体系的复杂巨系统特性，系统业务和使命、系统结构千差万别，简单的 5 类划分和共性基线不足以指导信息保障体系的建设，明确系统的个性功能和特殊保障需求是建设信息保障体系不可缺少的步骤。

位于同一级别的系统，对于保密性和可用性等安全属性的需求不一。以保密性 C 为例，对应着 5 组保障基线，每组保障基线由技术、管理和战略等保障要素来描述（见表 6-6）。

其中，$C_i=\{t_i,m_i,s_i\},1\leqslant i\leqslant 5,i\in N$ 表示第 i 级对保密性的保障需求，我们称之为对保密性的增强保障基线。增强保障基线由行业或系统自主确定。

表 6-6　增强保障基线（以保密性为例）

ABL / 等级	保密性			
	分类描述			ABL
	技术（T）	管理（M）	战略（S）	C
第一级（很低）	t_1	m_1	s_1	C_1
第二级（低）	t_2	m_2	s_2	C_2
第三级（中）	t_3	m_3	s_3	C_3
第四级（高）	t_4	m_4	s_4	C_4
第五级（很高）	t_5	m_5	s_5	C_5

增强保障基线实际上是对电子政务信息安全保障属性的精细描述，以此为基础可以对其所对应的安全域进行更详尽、更具体、更科学的描述，为电子政务信息资源共享和交互安全策略的制定提供依据。基于基线的安全域划分的另一个特点是动态性，随着系统业务的变化和不同时期使命的调整（如重要保障任务期），保障基线会随着保密性等安全保障目标的调整而调整，其安全保障策略也会随之做出动态的更新。

6.5.2　身份管理

在被研究的电子政务系统中往往涉及人的参与，即人担任管理决策和具体执行者的角色，或被管理对象中有人的参与。在很多情况下，人既是管理者又是被管理者，甚至可能是系统的破坏者，因此，人在不同管理层次中具有不同的身份。人的行为和参与极大程度地增加了系统的复杂性，给电子政务信息系统中人员的身份管理带来了很大的挑战。利用电子政务信息系统，政府部门之间可以通过网络来传输数据、交换数据、共享信息并实现协同办公，进而进行数据挖掘分析和决策支持，以便更好地管理社会和服务社会。在这些业务运行过程中，会有各种复杂角色的用户参与，建立这些用户的“电子身份”是十分必要的。对于这样复杂的系统，身份管理成为电子政务信息安全保障体系建设的一个基础性问题。这就需要建立一组与用户身份相对应的电子属性。对这些电子身份实施有效、有序管理对于提高行政效率、缩减行政成本、建设服务型政务具有重要的作用。

1．建立电子政务身份管理的统一框架

由于历史原因，在政府信息系统建设过程中，常常根据自身的情况采用不同的技术和体系结构来建立信息系统，这种跨平台的异构系统容易形成信息孤岛，给信息资源共享和业务协同带来了层层不便。统一的身份管理框架（见图 6-12）可以有效实现不同部门、不同地域的信息资源共享和相互访问，有效解决异构政务系统间的互操作问题。

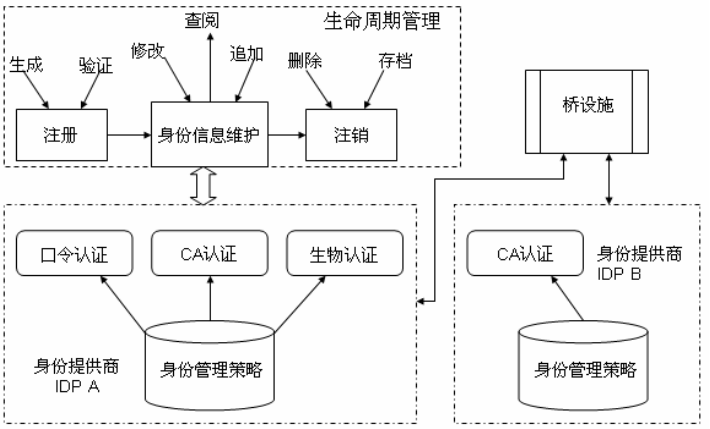


图 6-12　电子政务身份管理框架

电子政务身份管理主要涉及对用户身份信息的收集、存储、处理和散发等过程，这些信息都较为敏感，且涉及公民的隐私。电子政务身份管理应包含电子身份的注册、维护、注销等多个环节，在身份认证方面应提供多层次、多级别的按需认证机制，并通过桥设施实现全国电子政务身份管理的互操作性（见图 6-13）。

（1）认证策略

认证和保密是信息安全领域的两个重要内容。保密主要为了保证秘密信息的不可破译，而认证则用来获得对一个实体身份合法性或某一宣称的事实真实性进行证明的方法。认证主要有两个目的：一是验证信息发送者或系统访问者的身份的真实性，防止被冒充，以保证用户的合法性，此类目的的认证称为实体认证；二是保证信息传送过程中的完整性，以防止信息的篡改、重放等攻击。这里主要

讨论实体认证。在网络中的各种政务行为中，当某个实体声称自己具有一个特定的身份时，认证服务将利用某种策略来证明这一声明的正确性。认证主要包括以下策略。

- 基于口令的认证策略：口令是最为常见的一种认证机制，它通过验证声称者是否知道某事或某物来验证其身份的真实性。这种认证方法的优点在于，一般的系统都提供了对口令认证的支持，简单且易于实现。但同时也存在下面几点不足：每次访问系统时都要以明文方式输入口令，容易泄密；口令在传输过程中可能被截获；系统中所有用户的口令以文件形式存储在认证方，攻击者可以利用系统中存在的漏洞获取系统的口令文件；为了记忆的方便，不同安全级别的用户往往采用相同的口令，可通过猜测易被攻击的低安全级别系统的口令来对高安全级别系统进行攻击；只能进行单向认证，攻击者可以伪装成系统骗取用户的口令。
- 基于数字证书的认证策略：采用数字证书来证明身份具有安全、方便等优点，已经普遍被人们所接受。随着 PKI 桥认证和互操作性的研究，PKI 技术可以从个别企业的应用扩展到多个组织、整个国家甚至可以跨国家。数字证书的格式遵循 X.509 标准。X.509 是基于国际电信联盟（ITU-T）的公钥密码证书结构，其结构如图 6-13 所示。

图 6-13　X.509 版本 3 的证书结构

X.509 证书各个字段的含义如下。

① 版本号：该字段用于区分证书的版本，如版本 1、版本 2、版本 3。

② 证书序列号：证书颁发机构颁发证书时对每个证书的唯一编号。

③ 签名算法标识符：说明签名证书所使用的算法及相关参数。

④ 颁发者名称：该字段用于标识证书颁发机构的名称。

⑤ 有效期（不早于/不迟于）：该字段定义了证书的有限时间段，除非证书被撤销。该字段使用 UTC 时间或通用时间。

⑥ 主体名称：该字段用于表示证书的拥有者的特定名称，也就是拥有与证书中公钥所对应的私钥的主体。此字段必须为非空。

⑦ 主体公钥信息：该字段含有主体的公钥、算法标识符及算法所使用的任何相关参数。本字段必须有且仅有一个条目。

⑧ 颁发者唯一标识符：版本 2 或高于版本 2 的证书才含有此项，用以保证证书颁发机构的 X.509 名字没有二义性。

⑨ 主体唯一标识符：版本 2 或高于版本 2 的证书才含有此项，用以保证证书拥有者的 X.509 名字没有二义性。

⑩ 扩展项：版本 3 或高于版本 3 的证书才含有此项。该字段包括密钥和策略信息、主体和颁发者的属性，以及证书路径限制。

- 基于生物特征的认证策略：基于生物特征的认证方式以人体唯一的、可靠的、稳定的生物特征（如指纹、虹膜、脸部、掌纹等）为依据，采用计算机的强大功能和网络技术进行图像处理和模式识别。该技术具有很好的安全性、可靠性和有效性，与传统的身份确认手段相比，有着明显的优势。

（2）证书管理

- 注册：包括身份信息的声称和验证环节。
- 身份信息维护：包括已注册身份信息的修改、查阅和追加等环节。

- 注销：除非身份信息具有很短的生命周期，仅被有效地使用一次，否则就需要增加有身份信息的撤销和销毁等功能。

2．建设分布式、多级别电子政务认证服务中心

电子政务认证服务中心（Authentication Service Provider，ASP）是电子政务工程的重要组成部分。要实现跨部门、跨地区的信息资源共享，支持电子政务业务系统的互联互通和信息资源共享，必须建立统一管理的认证服务中心。认证服务中心包括电子政务门户和身份凭证服务提供商（Credential Service Providers，CSPs）。用户可以根据所需的服务选择相应的身份凭证，电子政务门户根据用户的申请把他导向相应的 CSP 进行认证。CSP 根据安全级别分为不同的安全等级，如基于 PIN/口令的弱认证和基于数字证书的强认证等。电子政务门户可以引导公民和企业在 CSP 处获取证书，并对用户进行认证，把通过认证的用户导向相应的政府站点以获取相应的政府服务。在电子政务门户，用户可以找到自己所需要的政府服务，并可以在这里申请认证以获取该项服务。通过认证服务中心，用户在政府服务站点之间进行切换时，不必进行重新认证。认证服务中心为公众和政府之间建立了在网络上交互的信任环境，拉近了公民和政府间的距离，使公民真正体会到随时随地可以获取政府服务的便利。

3．实现身份认证的互操作性

身份认证中的一个关键问题是如何实现互操作性。安全互操作性要求不同机构间使用不同的安全产品时，它们之间仍可以建立起信任关系。访问某个政府机构 A 并通过认证的用户，可以不需要再次认证就可以访问安全等级相同或较低的其他政府部门 B。因此，建设电子政务信息安全保障体系，强化互操作性管理势在必行。互操作性是实现互联互通的基础，通过认证的用户可以访问处于同一安全级别或较低级别的其他政务系统，而不需要进行重新认证，可以大大节约时间和费用。解决互操作性问题有两种途径：通过交叉认证或基于桥 CA（见图 6-12）。交叉认证用于相互独立的不同认证设施的两个节点 CA 之间，在这两个认证设施间建立起信任关系，实现两个认证设施之间的互操作性。桥 CA 则是通过一个可信的桥设施分别与两个独立的认证设施的根节点进行交叉认证，从而为这些根节点之间建立起信任关系。

6.5.3　敏感信息保护

1．敏感信息分类

在电子政务系统中，很多信息泄露和不当利用都是因为内部人员的违规操作、管理不当、无意中感染木马或病毒等造成的。政府信息敏感类型复杂多样，科学的分类是实现有效管理的基础。可以按照信息保密性的一般分类方式分类，也可以根据信息在具体应用环境下的特点进行分类。结合《中华人民共和国保守国家秘密法》的有关规定，国家秘密的密级分为绝密、机密、秘密三级[139]。本研究将政府信息按敏感程度分为 5 个类别：绝密类、机密类、秘密类、工作敏感类和开放公开类，这是信息的敏感性属性。这几类信息按共享环境又可分为条件共享类、强制共享类和不予共享类，这是信息的可共享性属性（见表 6-7）。

表 6-7　政务信息的敏感属性和共享属性标识

共享属性	敏感性	可共享性
某类信息	{绝密,机密,秘密,工作敏感,公开}	{无条件共享,条件共享,不共享}

其中，从政务信息的敏感性分析，可做如下界定。

① 绝密类、机密类、秘密类信息属于涉及国家秘密信息。2002 年 9 月 24 日，原国务院信息办在广州召开的全国电子政务建设地方座谈会上明确了政务内网是涉密网。2002 年 10 月，中保委〔2002〕4 号文件明确了政务内网是涉密网。2006 年 5 月，中办、国办转发的《国家信息化领导小组关于推进国家电子政务网络建设的意见》（中办发〔2006〕18 号）特别指出，涉及国家秘密的信息系统建设和管理，要严格按照党和国家的有关保密规定执行。

② 工作敏感类信息，是指由部门内部规定的涉及公民隐私、企业秘密等的非国家秘密信息。一旦这些信息被泄露（特别是批量泄露），就会造成不良后果和负面影响，损害公民、企业或部门声誉，可能带来不必要的经济损失。这些信息可

[139] 中华人民共和国主席令第二十八号《中华人民共和国保守国家秘密法》第十条，2010 年 10 月 1 日起实施。

运行在配置了安全防护策略的政务外网，如通过 VPN 等安全手段实现对信息的访问和处理。

③ 开放公开类，是指依据《信息公开条例》需要向社会公开的信息。这些信息在确保精确性、完整性、可用性的基础上可运行在政务外网或基于互联网的政务系统上。

从政务信息的可共享性分析，可将无条件共享、条件共享、不共享界定如下。

① 无条件共享：对于行政许可或跨部门并行审批的政务信息资源，可要求行政机关必须提供共享，如公共服务设施信息、社会经济统计信息等。

② 条件共享：对于与政府协同办公相关且信息内容较为敏感的信息资源，可按特定条件提供给相关行政部门共享的政务信息资源，即为条件共享类，如商业秘密、个人隐私信息及泄露后影响行政执法和政府政策办公的信息。

③ 不共享：对于有法律、法规或政府规章明确规定，不能提供给其他行政机关共享的政务信息资源，纳入不予共享类，如涉及国家秘密信息，应按国家有关保密规定处理。

敏感性和可共享性构成了政务信息管理的两大重要属性，通过对信息进行属性标记，可以实现电子政务信息在复杂环境下的运行、交换和共享。根据信息的敏感程度和共享性质就可以按需选择配置信息安全保障策略。

2．用户信息隐私保护

在敏感信息中，除了国家机密、商业秘密、工作秘密，还有一类个人隐私信息。根据我国的情况，个人数据的隐私敏感度大致可分为 4 级：① 无隐私性，如性别；② 一般隐私性，如姓名、出生日期、出生地、民族等；③ 较高隐私性，如居住地址、照片等；④ 高隐私性，主要包括财务状况、健康状况和儿童相关数据。

随着我国电子政务信息资源共享工作的不断深入开展，共享信息的类型不断增多，共享信息的范围不断增大，隐私保护带来的挑战愈发严峻。在信息资源共享的过程中，如何在保证电子政务业务完成的前提下有效地保护隐私信息，是研究安全的电子政务信息资源共享建设亟待解决的关键问题之一。

首先，我们从电子政务信息资源共享的三种模式入手，对隐私保护问题进行分析。

（1）政府与社会之间的信息资源共享

① 信息发布中的隐私保护问题。

在政府与社会之间的信息资源共享部分，政府通过发布信息来为公众服务。在信息发布中，如果不考虑信息披露的必要性和充分性界限，过度地披露了有关当事人的隐私信息，就会触犯当事人的合法利益，甚至使当事人在当地无法生活或无法生存。但是如果有些应当披露的信息不充分披露，就会让社会产生各种猜度，长此以往，就会使人民丧失对政府的信任。

② 电子政务资源使用过程中产生的数字行为等相关的隐私问题。

电子政务资源使用者包括个人用户和企业用户。在使用电子政务资源的过程中，如果对其产生的数字行为相关的隐私信息资源共享不当，就会对个人用户和企业用户的隐私带来安全威胁。

（2）政府部门之间的信息资源共享

政府部门之间共享信息资源、协作完成政府业务时，面临以下几类隐私保护问题：

① 数据挖掘中的隐私保护问题。

当政府业务需要从共享的数据中挖掘知识和信息来形成决策时，在保证业务完成的条件下需要对隐私信息进行保护。

② 信息资源共享过程中的推断隐私安全的问题。

各部门之间产生的共享数据集合中本身不包含隐私信息，但是通过共享数据集合可能推断出共享数据集合之外的隐私信息，这将带来隐私信息安全的问题。

③ 不同管理层级的机构对涉及隐私的信息保护力度不同产生的问题。

当高级别部门对涉及隐私的信息保护力度高于低级别部门时，如果高级别部

门与低级别部门共享相同层级（或敏感度）的隐私信息，信息得到的则是低级别的保护，将会对共享信息集合的安全造成威胁。

④ 平级管理机构与上下级管理机构在信息资源共享中权限的问题。

通常政府部门的高级别部门具有高于低级别部门的权限，但是平级部门之间对相同信息的权限可能不同。当高级别部门与多个平级别的低级别部门共享信息时，如果高级别部门暂时授予各个平级部门相同的权限，则会危害隐私信息安全。

⑤ 包含隐私的信息安全问题。

当共享包含隐私的数据时，将面临安全技术上的危险，如被窃听等盗取数据技术。

（3）政府机关内部的信息资源共享

对于政府机关内部涉及隐私信息的共享，可能会出现对隐私信息访问权限的授权管理不当带来的隐私信息安全威胁。

由于政府部门之间信息资源共享工作流程较为复杂，并且是电子政务信息资源共享建设工作的难点和重点，因此，我们重点研究政府部门之间信息资源共享中的隐私保护方法。

为解决政府部门之间信息资源共享中的隐私保护问题，本研究提出一个隐私保护模型。该模型由业务识别模块、数据预处理模块和业务协同模拟器三部分组成。业务识别模块用于识别电子政务信息资源共享的业务类别，包括以数据挖掘（或数据统计）技术来实现相关政务决策（简称业务 1）和通过共享信息来完成电子政务业务协同（简称业务 2）两种。数据预处理模块用于业务 1 之中，通过对共享信息中涉及的隐私信息的泛化预处理，保护在数据挖掘（或数据统计）产生决策的过程中涉及的相关隐私信息。业务协同模拟器用于业务 2 之中，其输入是实现业务协同的各个部门申请共享信息的属性组合，通过协同业务的小规模模拟并对比模拟器的输出，来确定实现协同业务所需共享的包含最少隐私信息的集合。隐私保护模型的体系结构如图 6-14 所示。

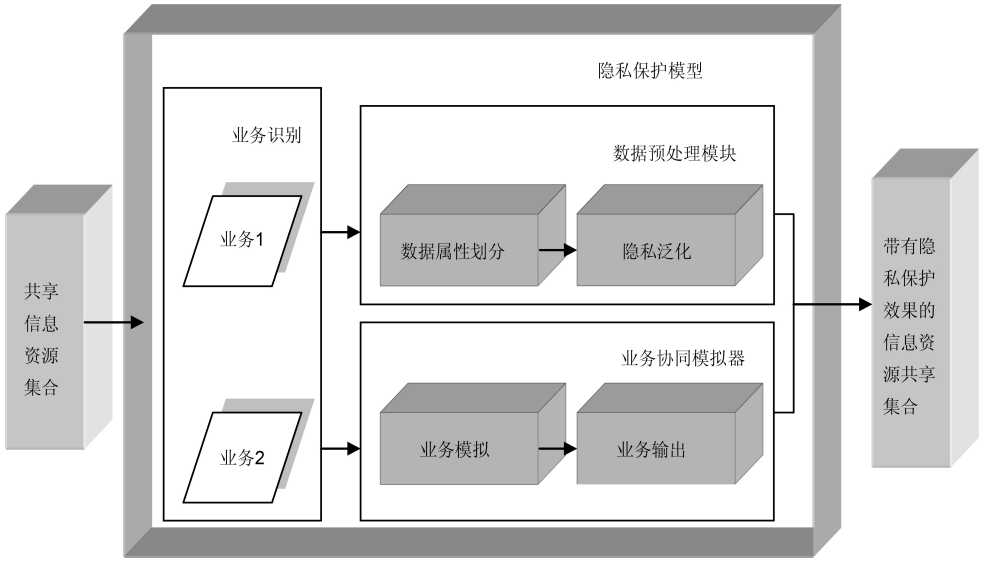


图 6-14　隐私保护模型

隐私保护模型的输入为电子政务信息资源共享集合，输出为具备隐私保护功效的新的信息资源共享集合。模型的应用流程包括以下步骤：

第一步，模型通过业务识别模块识别出信息资源共享的类别。

第二步，如果共享类别属于业务 1，则使用数据预处理模块对共享信息资源集合中的数据属性分类，根据分类结果进行隐私泛化处理，产生一个新的共享信息集合；否则，至第三步。

第三步，如果共享类别属于业务 2，则使用业务协同模拟器，通过对业务的小规模模拟找出不必要共享的隐私信息类别，产生一个确保业务实现且包含最少隐私信息的共享数据集合。

（1）数据预处理模块

业务 1 即以数据挖掘（或数据统计）技术来实现相关政务决策。面临的隐私问题包括保护隐私信息和保护数据表链接带来的推断隐私信息安全。数据预处理模块通过对隐私信息的泛化预处理，实现对隐私信息和数据表链接带来的推断隐私信息的保护。数据预处理模块的实现包括以下几个步骤：

第一步，划分数据属性。将共享的信息资源按照属性划分为标识符、准标识符、敏感属性和非敏感属性 4 种。

第二步，隐私泛化。对标识符、准标识符和敏感属性进行泛化处理，即将标识符存储在一张序号表之中（见表 6-8），在业务 1 的实现过程中，用序号代替该标识符；对于准标识符和敏感属性，采用匿名化的隐私保护技术对数据进行预处理。匿名化的隐私保护有多种方法和技术，如经典的 k-匿名方法、l-多样性原则、p-sensitive 的 k 匿名、(*α*,*k*)匿名、(*k*,*e*)匿名、t-closeness 匿名等技术[140]。在此不指定具体的匿名化技术，在实际应用中根据需要对共享的隐私信息选择合适的方法进行预处理。

表 6-8（1） 标识符编号

标识符	名称	序号
1	身份证号	A1,A2,…
2	姓名	B1,B2,…
…	…	…
n	…	N1,N2,…

表 6-8（2） 预处理后标识符

标识符	序号
1	A1,A2,…
2	B1,B2,…
…	…
n	N1,N2,…

经过数据预处理产生的新的数据集合，是对以数据挖掘（或数据统计）技术来实现相关政务决策过程中的隐私信息进行泛化的结果。新的数据集合能够保护隐私信息不因数据表链接而被推断，同时降低了隐私信息在共享过程中因人为、技术、或管理等因素带来的泄露风险，在一定程度上保护了隐私信息的安全。

[140] 王平水，王建东. 匿名化隐私保护技术研究综述[J]. 小型微型计算机系统，2011，32（2）.

（2）业务协同模拟器

业务 2 即通过共享信息来完成电子政务业务协同面临的隐私保护问题，这些问题突出表现为隐私信息资源共享过量，从而对隐私信息安全造成威胁。业务协同模拟器用于在保证电子政务业务协同完成的前提下，确定出包含最少隐私信息的共享集合。模拟器的实现包括以下几个步骤：

第一步，设各个部门准备共享信息资源的集合为 C，I 表示集合中的一行记录 $I\{i_1,i_2,\cdots,i_m\}(m\geqslant 1)$，其中，$i_j(1\leqslant j\leqslant m)$表示的是 I 中数据字段的类别（如姓名、身份证号等）。数据字段的类别属性共有 4 种，分别是标识符、准标识符、敏感属性和非敏感属性。

第二步，对于记录 I 中的数据字段类别，选取 $r(r\geqslant 1)$个数据字段进行业务协同模拟。输入 $I\{i_1,i_2,\cdots,i_m\}(m\geqslant 1)$中所有数据类别的子集合进行业务协同模拟（每种数据输入 r 条记录），即输入$\{(i_1),(i_2),\cdots,(i_m),(i_1,i_2),(i_1,i_3),\cdots,(i_1,i_2,\cdots,i_m)\}$（共有 C_m^m 种）。经过业务模拟后，如果某种输入能完成业务协同则记为 1；否则记为 0。

第三步，设经业务模拟后，输出为 1 的所有输入集合为 $INP\{\text{input}_1,\text{input}_2,\cdots,\text{input}_n\}$，其包含的数据类别分别为$\{(i_1,i_2,\cdots,i_r),\cdots,(i_1,i_2,\cdots,i_s)\}$。选取输入集合 INP 中包含标识符、准标识符和敏感属性最少的集合，作为新的信息资源共享集合。

经过模拟器产生的新的数据集合，能够确保在完成业务协同的前提下，共享包含最少隐私信息的集合，从而降低了隐私信息在共享过程中因人为、技术或管理等因素带来的泄露风险，在一定程度上保护了隐私信息的安全。

隐私保护模型将电子政务信息资源共享划分为基于数据挖掘或统计产生决策的业务和业务协同两类，分别采用数据预处理对隐私信息进行泛化和使用业务协同模拟器确定协同业务所需的最少隐私信息集合的方法，解决共享中的隐私保护问题。因此，隐私保护模型对于解决电子政务信息资源共享中的隐私保护问题具有一定的实际应用价值。

第 7 章

以大数据推进电子政务信息资源共享和安全保障的思路

全球大数据的蓬勃发展给我国提供了难得的发展机遇，在电子政务方面，大数据应用对电子政务的推动作用在一些发达国家已经得到证实。应用大数据一方面可以使我们更全面、更及时地认识客观世界；另一方面，大数据更加注重分析相关性，关注事物之间的普遍联系和规律。通过挖掘分析这些数据，能够使人们找到数据背后的真理，从而更好地认识事物的发展变化规律，提高政府决策的效率和精确性。因此，大数据作为一种新型的政府治理资源，为提高政府治理水平提供了新的渠道和手段。

7.1 大数据的概念及特点

由于大数据内容广泛且出现时间较短，目前对于大数据还没有十分明确的标准化定义，一般认为大数据是一种数据量巨大、数据形式多样、数据结构复杂的非结构化数据。麦肯锡全球研究所给出的定义是：大数据是一种规模大到在获取、存储、管理、分析方面大大超出了传统数据库软件工具能力范围的数据集合，具有海量的数据规模、快速的数据流转、多样的数据类型和价值密度低四大特征[141]；维基百科给出的定义是：巨量资料或称大数据指的是所涉及的资料量规模巨大到无法通过目前主流的软件工具，在合理的时间内达到撷取、管理、处理并整理成为帮助企业经营决策更积极目的的资讯[142]。百度百科给出的大数据定义是：大数据（Big Data）指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合，是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力来适应海量、高增长率和多样化的信息资产[143]。

IDC 给出了大数据的四个特点，即数据规模大（Volume）、数据种类多（Variety）、数据要求快速响应（Velocity）、数据价值密度低（Value），即所谓的“四V”特性，这些特性使大数据区别于传统数据。

1．数据规模大

数据规模大是大数据最基本的特征。随着互联网的广泛使用和信息技术的发展，使用互联网的企业和个人增加，用户获取数据更加便利且渠道更加多元化，而用户在使用互联网过程中的浏览痕迹也成为大数据的一部分。大数据通过对海量数据的搜集、处理和分析，可以使对事物的研究更加精确化和细节化，可以更好地描述事物属性。

---

[141] 麦肯锡全球研究所报告 *Big data: The next frontier for innovation, competition and productivity*，2011.

[142] http://www.36dsj.com/archives/6255。

[143] 引自百度百科“大数据”定义。

2．数据种类多

在网络不发达的时代，互联网上的结构化数据占多数，在存储数据前需要先构造数据结构，而新产生的数据可以根据其属性进行分类，然后存储在合适的位置。在这种情况下，数据的存储、处理和查询都较为简单。随着互联网上非结构化数据呈指数级增长，半结构化和非结构化数据已经成为主流，以往对数据进行分类然后存储的方法不再适用，大数据作为一种主要处理非结构化数据的方法逐渐成为信息处理领域发展的导向。

3．数据要求快速响应

数据的快速处理是大数据的重要特征之一，也是大数据和海量数据最大的区别。大数据意味着数据规模巨大，如果数据没有及时得到处理，则会加重网络负担，数据也没有得到充分利用，大量数据将失去价值。如今，互联网上每天都会产生大量数据，能够实时处理新增数据也是对大数据的基本要求之一。

4．数据价值密度低

数据价值密度低的特点是和大数据的非结构化特征相联系的。传统的结构化数据在对数据进行存储前会选择对描述事物有用的信息，处理后的数据中包含数据的属性和特征；而大数据则不对数据进行采样和选择，而是直接使用全部数据。由于没有剔除数据的过程，因而大数据可以分析更多的信息，可以更加全面地描述事物细节；但大数据也引入了大量对事物描述没有价值的信息，而这些信息占据了巨大的存储空间，所以相对于结构化数据，大数据使用的非结构化数据的价值密度较低。

7.2　大数据时代的电子政务发展现状

近两年来，各级政府逐渐重视大数据对于电子政府的推动作用，从政策指导和具体实施方面为大数据在电子政务领域的应用创造了良好的条件。

1．大数据在电子政务领域应用的宏观政策环境不断完善

随着互联网和信息技术的发展，电子政务的重要性愈加突显，大数据的出现及其在电子政务领域的运用有效地促进了政府信息资源的开放和共享。近年来，政府出台了众多政策来推动电子政务的发展和大数据在电子政务中的应用。

2012 年 2 月，《国家电子政务“十二五”规划》提出，在“十二五”期间要完成以云计算为基础的电子政务公共平台顶层设计；制定云计算基础上的电子政务框架，规范云计算的标准；开展电子政务公共平台的试点工作，在总结经验的基础上进行推广。

2012 年 5 月，《“十二五”国家政务信息化工程建设规划》中分析了我国政务信息化工程建设的现状，并将构建电子政务网络作为信息化工程建设的重点项目之一。政务信息化工程的建设有助于完善基础设施、培养信息技术人才，为大数据在电子政务领域的应用创造条件。

2012 年 7 月印发的《“十二五”国家战略性新兴产业发展规划》将信息感知技术、信息传输技术、信息处理技术和信息安全技术列为四项关键性的技术创新工程，信息处理技术中包括海量数据存储、数据挖掘、图像视频智能分析；还提出要加快建设下一代信息网络，推进云计算等新一代信息技术的发展。

2013 年，科技部将大数据列入“973”基础研究计划，在“973”计划的支持下，“网络信息空间大数据计算理论”和“网络大数据计算的基础理论及其应用研究”项目于 2014 年开始实施。

2013 年 1 月 11 日，工业和信息化部发布了《关于数据中心建设布局的指导意见》，提出科学推动数据中心建设和布局的指导思想及基本原则，对数据中心的规模进行了划分，并对新建超大数据中心、大型数据中心、中小型数据中心和已建数据中心进行布局导向，还提出了数据中心建设布局的五项保障措施。

2013 年 6 月，工业和信息化部发布了《电信和互联网用户个人信息保护规定》，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》，提出了信息搜集和使用的规范，明确了个人信息的安全保障措施和监督机制，为大数据应用过程中的个人信息保护提供了法律保障。

2014 年 11 月，《关于促进电子政务协调发展的指导意见》明确提出要利用五年时间，使电子政务在国家治理体系和治理能力现代化建设中发挥重要作用，同时提出要推进信息资源的共享和开放利用，切实加强信息资源的安全保障工作。

2014 年《政府工作报告》明确提出，“以创新支撑和引领经济结构优化升级”，“大力推进创新。创新是经济结构调整优化的原动力。要把创新摆在国家发展全局的核心位置，促进科技与经济社会发展紧密结合，推动我国产业向全球价值链高端跃升”。大数据是互联网领域的创新，而推动大数据在电子政务方面的应用也是电子政务的一种创新[144]。

2015 年 1 月，国务院发布《关于促进云计算创新发展培育信息产业新业态的意见》，提出要增强云计算的服务能力和创新能力；探索电子政务云计算发展新模式，鼓励使用云计算技术来整合政府信息资源；促进大数据在电子政务中的运用，推动政务信息资源融合与共享。

2015 年 8 月 19 日，国务院通过了《关于促进大数据发展的行动纲要》，这是目前我国大数据发展中极为重要的指导性文件。文件中提出要推动政府数据资源的共享，利用国家的电子政务网络，建立起联系各政府部门的统一信息资源共享和交换平台；推动大数据统筹工作的进行，依托现有的信息资源，加强资源整合，在中央层面上构建统一的互联网政务数据服务平台；通过运用云计算技术，整合较为分散的数据中心资源，形成规模合理、效率较高的政务数据中心体系；利用大数据来提高政府行政效率，简政放权，完善大数据监督和技术反腐体系，助力廉洁政府的建设；将大数据技术应用到医疗、教育、文化和社会保障等公共服务中，使政府服务更加精准[145]。

2016 年 4 月 14 日，国务院转发了国家发展和改革委员会等部门《推进“互联网+政务服务”开展信息惠民试点实施方案》，提出推进“互联网+政务服务”，促进部门间信息共享，是深化简政放权、放管结合、优化服务改革的重要内容。为进一步推动部门间政务服务相互衔接、协同联动，打破信息孤岛，变“群众跑

[144] 引自 2014 年《政府工作报告》。

[145] 引自《关于促进大数据发展的行动纲要》（国发〔2015〕50 号）。

腿”为“信息跑路”，变“群众来回跑”为“部门协同办”，变被动服务为主动服务，特制定本实施方案。

2．大数据在地方电子政务领域的实践

近年来，地方政府愈加重视大数据在电子政务中的应用，发布了诸多有关大数据应用和发展的意见，成立了大数据管理机构，在政府管理创新和智慧城市建设中得到了实践应用。

第一，制定地方性的信息资源共享政策。

2008 年 6 月，北京市信息化工作办公室印发《北京市政务信息资源共享交换平台管理办法（试行）》，提出了规范北京市共享交换平台的核心是建立目录中心，同时还需建设一个交换中心和多个交换节点。

2012 年 9 月，江苏省人民政府办公厅印发《江苏省政府信息化服务管理办法》，提出要推动跨地区和跨部门的信息资源共享，同时要加强信息化的统筹管理，建立统一的信息资源共享平台。

2014 年 11 月，浙江省人民政府办公厅印发《浙江政务服务网信息资源共享管理暂行办法》，规定了信息的共享类别，制定了信息采集的标准。

2014 年 12 月，海南省人民政府办公厅印发《海南省政务信息资源共享管理办法》，确立了政务信息资源共享的过程和标准，同时制定了信息共享的监督机制和问责机制。

2015 年 1 月，山东省人民政府办公厅印发《山东省政务信息资源共享管理办法》，提出要建立共享平台的政务信息资源基础数据库和共享主体数据库。

2015 年 5 月，河北省人民政府印发《河北省人民政府关于促进云计算创新发展培育信息产业新业态的实施意见》，重点建设能够提升云计算服务能力和创新能力的工程，利用云模式促进数据资源的开发和共享；同年 11 月，河北省人民政府又印发《河北省政务信息资源共享管理规定》，提出要建立省级的信息资源管理机构，加强信息共享基础设施的建设，并提出了关于政务信息资源共享的安全保障措施。

2015 年 6 月，天津市工业和信息化委公布了《天津市推进智慧城市建设行动计划（2015—2017 年）》，提出推行云计算模式，促进电子政务一体化，促进信息资源的共享和开发利用。

2016 年 1 月，《河北省政务信息资源共享管理规定》开始施行，提出要整合各类政府信息平台，提高政务信息资源使用效率，加强部门间的协调运作。

2016 年 2 月，上海市人民政府印发《上海市政务数据资源共享管理办法》，提出了建立数据资源共享平台的具体措施，并给出了数据资源目录、数据采集的方法和原则、数据使用的方法和原则，明确了数据资源共享的安全保障机制和监督机制。

第二，成立大数据管理机构。

“大数据管理局”的概念最早是由广州市提出的。2014 年 2 月 26 日，广东省人民政府印发《广东省经济和信息化委员会主要职责内设机构和人员编制规定》，决定成立广东省经济和信息化委员会，下设广东省大数据管理局，并且规定了大数据管理局的九项基本职责：研究拟订并组织实施大数据战略、规划和政策措施，引导和推动大数据研究和应用工作；组织制定大数据收集、管理、开放、应用等标准规范；推动形成全社会大数据形成机制的建立和开发应用；承担企业情况综合工作，负责企业数据收集和存储；组织编制电子政务建设规划并组织实施；组织协调政务信息资源共享；组织协调省级重大电子政务项目建设，组织协调网上办事大厅等电子政务一站式服务建设；负责统筹政务信息网络系统、政务数据中心的建设、管理；统筹协调信息安全保障体系建设；承担信息安全等级保护、应急协调和数字认证相关工作[146]。

2014 年 5 月，广东省佛山市南海区成立数据统筹局；之后，广东省清远市在其经济和信息化局的“三定方案”中要求设立大数据管理科。

2015 年 5 月，广州市人民政府公布了工业和信息化委员会、商业委员会和国有资产监督管理委员会的“三定方案”，决定成立广州市大数据管理局。

[146] 引自《广东省经济和信息化委员会主要职责内设机构和人员编制规定》。

2015 年 6 月，沈阳市大数据管理局成立，下设大数据产业处、标准与应用处和数据资源处。其主要职责是负责组织制定智慧沈阳的总体规划和实施方案；研究制定大数据战略、规划和相关政策；组织制定大数据的标准体系和考核体系，统筹推动全社会大数据库建设，组织制定大数据采集、管理、开放、交易、应用等标准规范；指导大数据产业发展；研究制定全市电子政务建设的总体规划、实施方案并组织实施；组织协调政务信息资源共享；统筹协调信息安全保障体系建设等工作[147]。

2015 年 9 月，成都市大数据管理局成立，大数据管理局为市经济和信息化委员会直属的正处级行政机构，主要职责是负责拟订全市大数据战略、规划和政策措施并组织实施；组织制定大数据收集、管理、开放、应用等标准规范，推动信息数据资源和基础设施建设的互联互通、资源共享；制定全市电子政务建设的总体规划并组织实施，牵头组织电子政务项目审核工作；推进电子政务外网现有信息系统整合，组织协调全市信息安全保障体系建设；成都市信息化工作领导小组办公室的日常工作[148]。

2015 年 11 月，黄石市大数据管理局成立，成为湖北省首个大数据管理局。其主要目标是建立民生数据中心、大商务数据中心、工业数据中心和政务数据中心。

2016 年 2 月，上海市大数据研究中心专委会成立，致力于互联网和大数据技术方面的突破，促进大数据成果向产业转移和扩散。

第三，政府信息资源开放和共享。

2012 年 10 月，北京市政务数据资源网试运行，企业和个人可以在该网站下载各种公开数据，为企业和个人提供了获取信息资源的新渠道，推动电子政务信息资源的开放和共享。

同年，上海市推出了上海政府数据服务网。该网站是国内首个政府数据服务网站，为公众提供经济建设、资源环境、教育科技、道路交通、卫生健康、城市建设等多个领域的数据。

[147] 引自中国沈阳市政府网站。

[148] 引自中国成都市政府网站。

案例 1：上海市徐汇区以大数据应用推进政务数据共享工作

徐汇区行政服务中心以数据共享为基础，加强互联互通，完善网上网下一体化建设。

一是推进网上政务大厅建设。运用大数据、云计算手段，将市工商、质监、房管、税务等 12 条专网、71 个市区联动业务系统、2 个区自建系统接入数据中心，建立数据信息“市区联动、全区共享”、“一次采集、多次利用、多方利用”机制。通过信息共享，打破数据壁垒，减少“循环证明、奇葩证明”，企业在设立阶段实际申报信息减少一半，申报材料压缩 1/3。审批事项、办事指南、表格下载、网上预约、网上反馈覆盖率实现 100%，网上填报覆盖率达 75%，现场接待量比预计减少 30%。

二是推进线上服务渗透率和实际使用率。开通网站、微信、APP 等网络服务渠道，提供在线、互动、多样、便利的行政服务，打造“一站式服务门户”。实体大厅月均接待量为 6 万人次，网站、微信月均访问量则突破 45 万次。

三是推行全程网上办理。实现“三证合一”换证、“优秀历史建筑装修改造申请”、“企业经营范围变更”、“企业开业名称核准”和“医疗废物产生申报”的全程网上办理，为下一步复制推广全程网上办理事项形成了基本经验。

四是完善企业服务“随心选”平台。以企业需求为导向，借助社会力量开展网上服务，引入中智、百事通、领英、惠众运营、慧家等业内标杆服务机构，为注册地在徐汇区的企业提供免费的口袋律师、智能人事代理、移动 OA、人才招聘、市场推广、房产咨询、员工住房等专业高效服务，切实降低中小企业发展运营成本。2016 年上半年已有 190 余家中小企业申请了此项服务并反馈良好。

五是网上网下联动发展。探索建立以行政相对人为中心的政务服务知识管理体系，设立咨询“单一窗口”，为办事群众提供全方位的咨询服务。中心建成一年零三个月以来，累计接待群众 89 万人次，网站、微信访问量突破 623 万次，整体满意率达 99.99%，实现了网下做实、网上做优。

资料来源：上海市徐汇区行政服务中心。

第四，建立大数据中心和产业园。

2013 年 1 月，国内首家大数据产业园——西咸大数据处理与服务产业园开工

建设。园区将从人口信息、电子政务、林业信息化、超算中心等方面全面开展园区建设，努力将西咸大数据处理与服务产业园建设成为西部最大的大数据处理和服务基地。按照规划，到 2020 年，西咸大数据处理与服务产业园将成为国家级的信息产业基地。

2015 年 2 月 25 日，国家级贵阳·贵安大数据产业发展集聚区创建授牌仪式在贵阳市举行，标志着我国首个国家级的大数据集聚发展试点示范区成立。2016 年 7 月 11 日，贵阳市通过了《中共贵阳市委关于以大数据为引领加快打造创新型中心城市的意见》，提出打造创新型中心城市的“一个核心、三大任务、四大支撑、五大保障”。

第五，大数据在建设智慧城市方面的应用。

在治理污染方面，2006 年，公共环境研究中心建立了国内首个公益性的水污染和空气污染数据库，通过该数据库，用户可以检索当地的水质信息、污染排放信息和污染源信息，也可以查询超标排放企业和污水处理厂信息。

在交通出行方面，2014 年 3 月，湖南省株洲市引入我国首个“高速铁路车辆网大数据和应用中心”，该项目基于大数据来分析铁路运行状况，为城市交通发展提供助力。

在城市规划方面，聊城市规划局使用城市三维辅助决策系统来对城市进行设计和规划，采用 Oracle 与 ArcSDE 相结合的空间数据库，整合了三维建筑模型数据、地上建筑、地表地物、地名标注、道路路网、数字正射影像图（DOM）、数字高程模型（DEM）、城市地下管线二三维数据等海量空间数据，为城市规划更为直观的表现方式。

7.3 大数据应用对于电子政务的意义

大数据是一种技术创新，可以拓展政府的信息渠道，减少政府各部门之间信息孤立的现象，同时可以增加公众对政务的参与度，提高政府决策的科学性。当

然，大数据作为互联网技术快速发展的成果，本身也存在一些漏洞，而且目前的大数据技术也有待完善，但总体而言，大数据在电子政务领域的应用利大于弊。随着大数据技术的成熟，大数据对于电子政务的推动作用将会越来越显著。

1．提高政府决策的科学化水平

目前，越来越多的政府部门开始摒弃以往根据经验来做出决策的方法，逐渐依赖电子政务的数据分析来进行决策。大数据提高政府决策的科学化水平可以从两个角度分析。

第一，大数据不仅可以对结构化数据进行处理，还可以对非结构化数据进行挖掘，在海量数据中提取有效信息，制作出直观可视的图表，这是以往的数据分析方法所不能完成的。大数据通过对不同数据的快速分析，可以更为准确地描述事物，为政府决策提供充分的信息和资源。

第二，大数据可以分析更多类型和数量的数据，极大地拓展了政府决策的信息边界，为政府决策提供了新的思路和方法，同时也为政府进行更为精准的决策提供了技术支持，让政府决策有据可依。

2．促进部门之间的信息共享和协调运作

以往各政府部门不愿意将自己掌握的信息资源与其他部门共享，这是由于该部门在搜集、整理信息时耗费了大量的人力、物力和财力，也可能是由于该部门害怕数据共享以后产生不良后果而需要承担责任。大数据的应用可以从两个方面促进政府部门间的信息共享和协调运作。

第一，大数据可以促使政府部门间进行信息资源共享及政府对企业和个人的信息开放，有助于减少“信息孤岛”现象，使信息资源的流动和处理更为流畅，增强部门间的协调性。

第二，大数据也可以提高数据的处理效率，提高政府部门的工作效率，降低政府运行成本。

3．提高公众参与度，增加政务透明度

大数据平台的建立为公众和政府之间的互动提供了一些新的渠道，既有助于

公众的参与，又可以加强公众对政府的监督力度。

第一，大数据可以推进电子政务的发展，提高数据的开放性和流动性。公众可以通过更多的渠道获取政府数据，并对政府决策提出意见和建议，增加了政府和公众之间的交流，提高了决策的公众参与度。

第二，大数据可以激发公众的创造性。公众在获取政府公布的数据之后，可以对数据进行再加工，从中获取更多信息，然后将这些信息反馈给政府，有助于政府部门集思广益，获得更多的有效信息。

第三，在大数据的推动下，政府会公开更多的信息资源供公众查询和使用，在这一过程中，公众可以监督政府的工作，促使政府的管理和服务更加透明。

4．提升政府的公共服务水平

建设服务型政府是我国政府部门转型的主要目标，大数据可以推动政府职能从管理向治理转变，可以从两个方面来谈。

第一，通过大数据分析，政府可以更详细和准确地了解公众的实际需求，对症下药，将当前的社会问题分开主次，解决公众最需要解决的问题。这不仅有利于政府工作的进行，同时可以更好地满足公众的需求。

第二，大数据可以帮助政府检验实际工作的成效，可以使政府根据大数据的分析结果及时调整、纠正工作内容和方法。同时，政府也可以根据数据分析结果有针对性地提升公共服务水平，使政府服务更加精细化，提升公众对政府服务的满意度。

5．有助于政府信息资源的安全保障

政府的信息资源数量多，而且其中很大一部分具有保密性。在信息时代，在提高信息资源利用效率的同时，如何保证信息资源的安全性成为政府面临的重要课题之一。大数据对于信息安全保障方面的作用可以从两个角度来分析。

第一，在大数据背景下，政府部门会对“信息安全”重新定义，扩展其内涵，同时重新确定信息的安全等级。大数据可以帮助政府对数据进行分级，选择可以共享的信息，从而保障个人隐私和国家信息的安全。

第二，通过大数据的分析，政府可以尽快发现系统漏洞，采取措施进行安全防卫；还可以根据数据分析结果来构建更有力的安全防护系统，提升电子政务的信息安全保障能力。

6．创新政府信息资源共享和安全保障的手段

大数据使政府部门可以采用更为多样化的方法进行信息资源的共享和安全保障，拓展政府部门之间、政府和企业之间、政府和个人之间的信息共享渠道。

第一，云模式是促进信息资源共享的全新业态，使得大数据在电子政务方面的应用落到实处。通过云计算，政府可以实时处理海量数据，做出更加科学有效的决策。云计算已经逐渐成为大数据处理和运用的基本框架，为大数据的存储、处理和分析提供了平台。

第二，在大数据背景下，政府可以通过更为广泛和灵活地使用互联网中的数据，获得更为准确的信息和资源；也可以建立更为完善的信息资源共享平台，建立更加有力的信息资源保障体系。

7.4　以大数据推进电子政务信息资源共享和安全保障的思路

在电子政务中，信息资源的共享和安全保障是两大重点，也是目前我国电子政务的薄弱环节。在大数据背景下，如何使用大数据来推进电子政务信息资源共享和安全保障是一种创新。本节提出以大数据推进电子政务信息资源共享和安全保障的几点思路。

1．制定大数据适用的法律法规

政府数据具有特殊性，一方面关乎个人的隐私安全，另一方面关系到国家安全，所以在政府数据开放和信息资源共享中，要更加关注共享的规范性和安全性。另外，由于政府关键数据泄露以后后果的严重性和政府部门较强的自我

保护意识，一些部门不愿将自己的信息资源与其他部门、企业和个人共享。基于以上两点考虑，国家在制定大数据在电子政务领域适用的法律法规时要重点关注两个方面。

第一，规范大数据在信息资源共享中的应用程序，保障数据搜集、处理和分析等各个阶段数据的安全性，只有在保证数据安全的基础上才能进行数据的开放和共享。

第二，从法律的层面对政府的信息资源共享做出明确规定，减少各部门因过度保护而阻碍信息共享的现象，建立政府部门信息共享的激励机制，从制度上确立信息资源共享在电子政务中的地位。只有政府部门合法、规范地公开和共享数据，大数据在电子政务领域的应用才有坚实的基础。

2．制定大数据背景下数据的安全类别评测

政府掌握的数据涉及个人隐私和国家安全两个方面，不同数据的保密性和价值也不同，所以在数据资源的共享上要有选择地开放。在大数据背景下，对事物的分析需要有大量数据作为基础，但也要明确数据使用时的等级，对数据进行安全类别的评测，根据评测结果来进行不同方式的数据处理。

政府应以法律形式对数据的安全类别做出规定，对不同类别数据的共享内容、共享形式和共享时间执行严格的程序。这有利于电子政务信息资源的共享和安全保障，指导政府数据资源的开发和保护。

3．促进电子政务领域大数据技术的创新

目前我国电子政务应用中的一部分关键设备仍从国外进口，对国外技术的依赖性较强，同时，我国的大数据技术发展也处于起步阶段，这加大了我国电子政务信息资源共享面临的风险。加强对大数据基础领域的研究，在综合数学、物理等多学科知识的基础上完善大数据的科学体系，探索大数据在电子政务领域应用的模型。

4．加强大数据背景下电子政务方面专业人才的培养

在大数据出现以前，互联网的使用还较为简单，数据的处理量也较少。如今，

随着互联网和大数据的发展，数据海量增加，数据结构也更为复杂，数据的处理难度加大，这就要求具有这方面专业知识和技能的人才来对电子政务的信息资源进行处理。对此，提出两点建议：

第一，建立多层级、多类型的大数据人才培养机制，鼓励高校开设相关专业和课程，鼓励高校培养跨学科的、具备统计分析和计算机技术等多种能力的复合型人才。

第二，鼓励高校和企业加强沟通合作，加强人才在企业的培养和锻炼，培育大数据技术和实用技能均具备的创新型人才。

第三，要加强电子政务方面专业人才的培养，使其能够适应大数据时代复杂多变的环境，对信息资源做出合理且实时的处理，这样才能提高电子政务信息资源共享的水平，保障信息资源的安全性。

5．提高大数据背景下电子政务的公共化服务水平

发展电子政务和鼓励信息资源共享的根本目的是提高政府的公共服务水平，提高政府在城乡建设、医疗保障、养老服务、劳动保障、社会就业、文化教育、城乡服务和交通旅游等方面的服务能力。大数据的应用可以为政府提高社会化服务水平提供新的渠道，促使政府加快完善服务体制和机制。

第一，推进社会保障领域的大数据化。政府可以利用大数据建立城乡统一的社会救济、社会福利和社会保障的电子政务平台，加强各部门之间信息的交流和共享，为真正需要社会保障的人群提供“安全网”，促进社会服务均等化，同时也可以提高财政资金在社会保障方面的使用效率。

第二，推进医疗服务的大数据。建立全国性的健康档案系统，完善健康信息的互联互通机制，建设覆盖城乡的医疗服务大数据体系，为公众提供更为及时、有效的医疗服务。

第三，推进交通服务的大数据。建立联合交通、气象、测绘等多部门的交通服务大数据平台，加强各地区的交通信息资源共享，利用交通大数据为公众提供更加精准化的交通服务。

第四，推进农业服务的大数据。通过大数据在农业领域的应用，构建联系农业、气象、地质等多部门的农业大数据体系，提高农业决策的科学化水平和农业生产的智能化水平，为农民创收提供保障。

6．处理好电子政务信息资源共享和安全的关系

电子政务信息资源共享是一把“双刃剑”，一方面，信息共享可以带来巨大的经济效益和社会效益；另一方面，共享的程度越高，意味着越多的信息资源开放，也意味着信息资源遭受攻击的可能性越大，信息安全面临的威胁越多。共享和安全是不可分割的一个整体的两面。

首先，信息安全是进行信息资源共享的前提和条件。只有在保证信息资源安全的情况下，才能进行信息资源共享。所以，进行数据等级划分是关键，要确保关键信息的安全性。

其次，共享是在确保信息安全下电子政务发展的必由之路。电子政务的发展要求政府必须提高信息资源共享的水平。在大数据背景下，信息资源共享已经成为提高政府服务能力所必须采取的措施。

第 8 章

健全我国电子政务信息资源共享安全保障机制的政策建议

电子政务信息资源共享是政府在信息时代创造、采集、分析、利用和传播信息的系统工程，是通过政府管理手段的创新，对政府职能、决策方式、管理行为、运行模式和工作流程进行改革和调整，以提高政府管理和服务的水平。而信息安全保障机制建设是促进电子政务信息资源共享顺利实施的保证，是推动政府信息化健康发展的基石。“十二五”时期提出，要大力推进电子政务建设，推动重要政务信息系统的互联互通、信息资源共享和业务协同。同时，要健全网络与信息安全法律法规，完善信息安全标准体系和认证认可体系；推进信息安全保密基础设施建设，构建信息安全保密防护体系；加强互联网管理，确保国家网络和信息安

全。针对当前我国电子政务信息资源共享和安全保障机制建设中存在的深层次问题，以第 6 章的理论模型和保障机制研究为基础，结合国际经验和“十二五”时期的新要求，围绕战略保障机制、管理保障机制和技术保障机制三个维度，提出如下建议。

8.1 加强战略统筹

1．重视战略，加强研究

要组织和整合专门研究力量，推进电子政务和信息安全战略研究，在战略层面确立电子政务信息资源共享和安全保障工作建设的原则。要研究分析与我国经济社会发展和大国崛起目标相适应的电子政务发展趋势和要求，提出电子政务信息资源共享和安全保障的目标和任务，为中央推进电子政务和信息化工作提供决策支持。要研究电子政务信息资源共享中存在的重大体制机制问题，借鉴和不断跟进发达国家和地区推进电子政务信息资源共享与安全保障的有益经验，提出未来电子政务信息资源共享和安全保障的顶层设计和实施方案。

2．加强统筹，统一规划

电子政务信息资源共享建设必须按照国家信息化领导小组的统一战略部署，制定总体规划，加强对各部门、各地区信息资源共享工作的指导。电子政务建设要充分利用已有的网络基础、业务系统和信息资源，加强整合，促进跨部门、跨地区的互联互通和信息资源共享，使有限的资源发挥最大效益。保障电子政务信息资源共建与共享，首先要保障共建与共享信息的安全，信息安全是电子政务信息资源共建与共享中最关键和最根本的问题。在国家信息安全法规、政策和方针的指导下，坚持积极防御、综合防范的方针，坚持信息安全保障与信息化同步规划、同步建设、同步发展。加快整合信息安全资源，统一规划建设电子政务应急响应系统和灾难备份系统，充分发挥各类信息安全基础设施的作用，形成以安全保共享、以共享促安全的良性循环机制。

3．完善标准，打破垄断

一是积极参与国际标准制定。加强信息安全技术标准化领域的合作交流，积极参与国际信息安全技术标准制定，提升我国在国际信息安全事务中的话语权。二是加快推进电子政务信息资源共享的基础标准、数据标准、交换标准、安全标准和管理标准的研制和宣贯，完善适合我国国情的电子政务信息资源共享标准体系。三是支持国内有实力的企业在掌握核心专利的基础上联合研制技术标准，突破发达国家对信息安全关键技术标准垄断的瓶颈。

8.2　实施顶层设计

1．加强政府信息资源开发利用

要满足政府、公众、企业的多样化、多层次信息需求，必须深化政府信息资源的开发层次。因此，要建立门类齐全、内容丰富、更新及时的数据库，做好专题性资源、预测性资源和创新性资源建设；对传统文献和电子信息资源进行整理整合，有针对性地编制二次文献（索引、目录）、三次文献（报告、综述），做好深度分析报告和支持政府决策的信息服务。为了高效、有序地共享和开发政府信息资源，政府部门需制订详细而周密的计划，确保政府所需信息资源的有效性和经济性。政府必须按照既定的程序，利用先进的信息技术手段，采用一体化的形式，有组织地收集、处理、传输、发布各种信息。同时，政府应当引入市场竞争机制来开发利用政府信息资源，以提高资源配置效率、增强经济发展实力。可选择委托、招标、外包、联合开发等模式，扩大非密集信息开发，鼓励信息服务企业对政府信息资源进行商业开发和提供增值服务。

2．确立电子政务信息资源共享的指导性原则

一是依法共享，即明确电子政务信息资源哪些可以共享、哪些不可以共享，以及共享双方所应承担的法律责任，这是信息资源共享工作能够顺利开展的基础。二是需求导向，就是要围绕经济和社会发展的重点和难点问题，按照建设服务型政府的要求，以政府信息资源共享不断扩大公共服务范围，逐步形成可持续发展

的电子政务公共服务体系。三是突出效益，就是要讲求实效，坚持经济效益和社会效益相统一，加强已有网络和信息资源的整合，避免重复建设，全面提升跨部门、跨地区业务系统的互联互通和协同，切实提高为公共服务、社会管理、市场监管和宏观调控服务的能力和水平。四是保障安全，就是要在推进信息资源共享的同时注意安全风险的防范，完善电子政务信息安全保障体系，提高信息安全保障能力，化解信息资源共享过程中产生的各种风险，创造一个良好的安全环境。

3．选择一批跨部门、跨地区的重大电子政务工程项目，实践信息资源共享和业务协同

一是以现有的国家电子政务基础网络为依托，建设国家级的电子政务信息资源共享平台，为各级政务部门开展跨地区、跨部门信息资源共享和业务协同提供支撑服务，为电子政务信息资源的开发和增值利用提供服务。二是加强地理、人口、法人、宏观经济等国家基础信息资源库建设，通过动态更新、联网比对，提高信息的真实性和准确性，不断推动其应用和共享水平。三是建设房地产、食品药品监管、企业信用等涉及国计民生的全国信息资源共享工程，加强信息综合利用，强化信息分析研判，进一步推进电子政务保障民生应用的积极作用。四是建设能源安全、环境监测、安全生产监管、应急维稳等全国信息资源共享工程，增强电子政务安全预警、辅助决策的作用，解决涉及国家经济社会安全的重点和难点问题，为公众提供和谐、平安的生产和生活环境。五是建设金融监管、价格监管、执法监督等辅助治国理政的全国信息资源共享工程，推进科学监管、动态跟踪、依法行政、文明执法，不断提高执政能力和管理水平。

4．对政府信息资源安全保障工作的设计

政府信息资源是重要的国家资产，信息资源共享和业务协同给电子政务信息安全保障带来很大的挑战，信息安全是政府信息资源开发和共享的重要保障。当前政府信息资源开发和共享的安全问题十分严重，这就迫切需要我们分析信息资源共享的安全威胁和风险，从战略、管理和技术三个维度来设计政府信息资源安全保障机制。信息资源安全保障机制包括以下几个方面：一是确立保障信息安全的整体策略，准确把握政府信息资源共享全局；二是建立健全信息安全管理体制，加强政府信息资源共享的安全管理；三是加强信息安全立法，提供政府信息资源

共享的法律保障；四是重视电子政务基础设施的安全防护，确保基础设施的安全；五是加强网络与信息安全技术的研发，提高政府信息资源共享的系统防护能力；六是加强有关方面的合作，构建政府信息资源共享的良好安全环境。

8.3　健全法律法规

1．加快推进《信息安全法》的出台

一是要深入研究《信息安全法》在整个法律体系中的地位和作用，以及与之相关的上下位法规之间的关联与互动，从国家层面分析信息安全法制层面需要解决的重大问题，设计提出信息安全法律法规体系的整体框架，分层次、有步骤地建立起适合我国国情的信息安全法律体系。二是立足于防范重大威胁，加强对重要领域信息系统的保护。将政府信息系统、基础信息网络和关系国计民生的重要信息系统的安全作为重点保护对象，提出安全防护的基本要求。三是明确信息安全工作责任追究机制。清晰界定信息安全工作中各方主体的权利和责任，形成各司其职、各负其责的工作局面，落实信息安全责任追究制度。四是对涉及的信息安全领域的国际协作做出规定，加强对跨国网络犯罪的取证、追踪和执法工作的协调，加强国际协作、合作与交流。

2．研究制定《个人信息保护法》

一是加强对个人信息保护立法工作的重视，切实提高对个人信息保护问题重要性、紧迫性的认识，提高对个人信息保护立法工作基础性作用的认识，建议尽快将《个人信息保护法》列入全国人大常委会法制工作委员会的立法计划，推动个人信息保护这一重大制度付诸实施。二是研究《个人信息保护法》的立法宗旨、基本概念、主管部门、基本原则、适用范围，合理界定个人信息保护的范围，明确个人信息保护的目标和原则。三是对个人信息采集主体、采集范围、采集程序、个人信息的存储与使用、更改程序、共享程序做出明确规定，规范个人信息的生产、存储和交换行为。四是界定网络环境下个人信息保护的范畴。对网络环境下个人信息的获取、存储、使用、披露和共享要有法律规范；明确合理使用与非法

滥用个人信息的界限；规定网络环境下个人信息受到侵害的诉求途径与法律责任；对网络环境下未成年个人信息制定特殊的保护条款。

3．研究制定《电子政务信息资源共享条例》

在针对“电子政务”的综合性法规难以于短期内出台的条件下，研究制定《电子政务信息资源共享条例》是解决当前政务信息资源共享难题的有效途径。在条例中明确政务信息资源共享的主管部门和各部门、各单位政务信息资源共享的责任、权利和义务，提出政务信息资源共享应当遵循的原则，研究各部门、各单位信息资源共享的范围、内容、方式和程序，建立政务信息资源共享长效机制，推动重点领域和跨部门政务信息资源共享。

8.4　完善管理体制

1．强化电子政务信息资源共享和安全保障的领导体制

电子政务成功实现的关键因素是强有力的领导机构的推动。作为一项复杂的系统工程，没有一个强有力的领导机构来发挥统领作用，电子政务信息资源共享工作很难推进。加强对电子政务工作的宏观领导和总体协调，健全跨部门协调机制，加强对电子政务重大事项的决策和协调，加强对电子政务信息资源共享推进情况的督促和检查，严格落实相关机构责任，按照“科学、公正、客观、实用”的原则，对国家电子政务信息资源共享工作实施情况进行绩效评估，评估结果作为项目预算投资的重要参考依据。明确信息资源共享中信息生命周期各个阶段的责任，建立一套完整的领导负责体制，彻底改变当前信息资源的所有方对信息资源共享带来的后续问题负责的现状，以调动各方共享信息资源的积极性。进一步理顺国家信息安全管理体制和协调机制，建立联席工作会议机制，切实加强跨部门安全保障工作的协调力度。

2．建立健全政务信息资源管理中心

一是在电子政务主管部门的指导下，整合现有资源，建立健全各级政务信息

资源管理中心，搭建电子政务信息资源共享工作专业化服务平台，为政务信息资源的共享、开发和增值提供服务。二是政务信息资源管理中心的目标：打破信息资源“部门割据”、“条块分割”的局面，协调推进信息资源共享工作；实现政府对电子政务资源的全程管理，降低管理成本，更好地提供公共服务。三是政务信息资源管理中心的主要职能：负责电子政务信息资源共享和交换平台的构建和运营；研究拟定信息资源的管理规范和技术标准；保障电子政务信息资源安全；为党政机关和社会提供信息咨询服务。

3．完善政务信息资源共享管理制度

一是建立政务信息资源分类共享制度。可将政务信息资源分为：可以无附加条件地给其他部门共享的为无条件共享类；按照设定条件提供给其他部门共享的为附加条件共享类；不能提供给其他部门共享的为不予共享类。对于无条件共享类政务信息资源，可通过政务信息资源中心自行获取。对于条件共享类，鼓励优先使用政务信息资源管理中心的信息资源共享平台进行信息资源共享的申请、评估和共享。对于特殊信息和特殊需求，允许信息使用者与拥有者直接共享。二是建立政务信息资源共享的申请登记制度。对于条件共享类信息，由信息需求方向信息提供方提出申请，共享申请需列明需要的信息、用途、共享可能产生的效益和使用依据。三是建立政务信息资源共享的专家联席评审制度。对于收到的信息资源共享申请，政务信息资源管理中心组织共享申请者、信息拥有者和有关专家进行联席评审，分析共享的法律依据和效益，确定是否共享。四是建立信息资源共享的绩效考核机制。主管部门应当根据各部门和各单位提供的共享信息数量来更新时效、频率及使用效益等，制定政务信息资源共享的绩效体系，定期对各部门和各单位的信息资源共享情况进行考核，并提出改进意见。

4．完善信息安全管理体制

加强国家网络与信息安全协调小组的领导，从战略层面加强信息安全管理，统一部署信息安全管理工作，充分发挥跨部门协调作用。进一步明确界定工信部、公安部、安全部、国家认监委、国家保密局、国家密码管理局等信息安全相关部门的职责权限，达到分工明确、各司其职、齐抓共管的目标。同时，在国家关键

部门和企事业单位中，明确地指定信息安全工作的职责和工作负责人，形成纵向到底、横向到边的信息安全管理体制。重视和加强信息安全等级保护工作，对重要信息安全产品实行强制性认证，特定领域用户必须明确采购通过认证的信息安全产品。

5．完善信息资源共享的安全保障工作机制

一是健全电子政务信息资源共享中的安全责任追究机制。清晰界定共享活动中各方主体的权利和责任，形成各司其职、各负其责的工作局面，落实信息安全责任追究制度。二是建立电子政务信息分级保障机制。对于无条件共享类、附加条件共享类和不予共享类，实施不同安全级别的分类保障。三是建立敏感信息处理制度。在满足政务信息资源共享要求的前提下，对可能涉及敏感内容的信息进行处理，例如对定量数据进行定性模糊处理或共享部分数据项等，避免直接共享完整数据可能带来的信息泄露等问题。

8.5　强化运行保障机制

1．强化电子政务资金保障机制

电子政务信息资源共建共享的实现离不开足够的资金投入，政府是实施电子政务的主体，各级政府要成为资金投入的主体力量，要为电子政务信息资源的共建共享提供足够的资金投入。按照“分级负担、共同建设”的原则，各级政府要将电子政务信息资源共建共享所需经费纳入本级政府的财政预算，省、市、县分别负担本级电子政务建设和运行维护所需资金，重点保障部门基础性业务、跨部门核心系统、公共基础设施和信息资源建设。对于涉及多个部门的信息资源共享互联互通工程建设，资金应统筹安排，公共部分的建设要设立专项经费予以保障。财政部门负责项目建设资金和运维资金的保障工作。在资金投入过程中，要切实加强资金管理，完善资金管理制度和资金使用的绩效考评制度，提高资金使用的规范性和有效性。

2．建立信息资源共享的市场机制

共建共享所需资金仅仅依靠政府的财政投入远远不够，还应在充分发挥中央和地方政府财政投入主导作用的同时，制定相应政策，充分调动科研院所、行业协会和企业的积极性，鼓励和引导社会资金参与电子政务信息资源共建共享系统工程建设、管理和运营。电子政务信息资源共建共享工程的建设和管理需要积极探索市场化运行模式，逐步向企业化、市场化运行方向转化，建议按照“谁投资谁受益”的原则建立协调电子政务信息资源共建共享供需双方利益的市场机制。鼓励政务部门尝试开展以电子政务信息资源共享建设为基础的增值服务，在保证国家安全的前提下，加大信息资源利用程度，以增值服务收入补贴信息资源共享建设，形成共享建设的良性循环。

3．建立健全产业扶持机制

国家要建立信息安全产业发展基金，采用项目贴息贷款、补助、奖励等方式滚动使用，用于电子政务、信息资源共享和信息安全关键技术、重点产品开发和产业化生产。同时鼓励风险投资，以此带动社会资本对信息安全行业的投资。允许通过多种渠道筹集资金，建立信息安全产业风险投资基金，并对其风险投资实行减免所得税等优惠政策。支持从事电子政务的企业在国内上市融资，采取比一般高科技企业更为优惠的政策。出台产业配套政策，重点扶持一批具有核心竞争力和国际竞争力的、产学研相结合的、具备自主创新能力的大型企业或企业集团。发挥国家级专业孵化器职能，鼓励创业和促进中小企业发展，做好服务工作，壮大产业基石。加强行业监管，规范市场秩序，营造公平的竞争环境，避免企业间的恶性竞争。充分发挥主管部门和行业协会的领导作用，打造确保信息安全的产业联盟。

4．完善人才培养机制

电子政务信息资源共享的安全保障离不开专业的技术人员，电子政务信息资源共享安全管理的核心要素是高素质的技术人才队伍。第一，建立和完善高校信息安全专业学科体系建设，加强课程设置和师资队伍建设，促进学、研、产、用各方面的紧密结合；依托电子政务专业机构及电信、移动等大型企业，建立相关

专业本科校外实习、实践基地。第二，高度重视专业人才队伍建设，创新人才使用机制，充分挖掘社会人才，逐步建立一支既懂管理又懂技术的人才队伍。第三，充分发挥各级各类教育培训机构的作用，切实有效地开展公务员电子政务知识、信息安全知识、电子政务技能等方面的培训。

8.6 推进新技术的应用

1. 以云计算技术推进电子政务信息资源共享向专业化、集约化和规模化发展

一方面，云计算作为网络资源共享利用的典型模式，其自身的特性决定了它能够有效减少电子政务信息资源共享的实现成本和扩大电子政务信息资源共享的范围，从而提高电子政务信息资源共享的效率；另一方面，云计算能够提供安全可靠的数据中心，便于对其进行统一的权限管理和有效的实时监测，降低电子政务信息资源共享的泄密风险，保障信息资源共享安全。因此，要加强研究和利用云计算技术推进电子政务信息资源共享模式的探索与创新。第一，要积极探索基于云计算的、既便于不同部门和单位共享电子政务信息资源又保障共享安全的电子政务信息资源中心构建模式。第二，研究利用云计算、虚拟化等新技术创新共享模式，对传统的孤岛型烟囱式系统进行虚拟化整合，提高政务信息资源和网络系统的利用率，降低运行成本。第三，搭建电子政务信息资源共享的云接入平台，并且做到搭建的接入平台既适用且容易接入，又能有效鉴别用户身份，防止非法操作和入侵等。第四，研究利用基于云平台的数据挖掘技术实现政务信息资源的整合和增值，提高政务信息资源的质量和开发利用效率。

2. 以云存储、云灾备技术推进电子政务信息资源灾备体系建设

相对于传统灾备技术异地备份的模式，云存储技术能够整合分散的数据存储和备份中心，以集中的数据资源存储和处理中心为整个系统提供不间断的服务，有助于构建一个具有高度业务连续性的电子政务信息资源共享环境。因此，要加强对云存储、云灾备技术的研究。第一，要探索和尝试云存储灾备解决方案，以成功案例推动云灾备技术的广泛应用；第二，要加强云存储安全技术的攻关，充

分利用云存储安全技术保证灾备建设和运维中电子政务信息资源的保密性、完整性、可追溯性等安全属性。

3．借助宽带移动通信和物联网技术加强社会管理

当前，宽带移动通信技术促成的移动办公、应急处理等电子政务新应用模式正逐步推广，物联网技术在医疗卫生、人口管理、社会治安、食品安全、交通运输等方面的综合应用也为推动社会管理创新提供了新的思路，加快了社会体制改革的步伐。因此，要加强对宽带移动通信、物联网等现代信息技术促进社会管理的研究。第一，要转变观念。要充分认识到通过信息化的新技术提升社会管理水平，高起点、高水平、高标准地规划好社会管理信息化，从而提高行政效率、增加政务透明度的重要性和必要性。第二，要大力推进宽带移动通信和物联网技术的研发和应用，充分发挥现代信息技术的优势，保障和改善民生，深化行政管理体制改革，充分履行社会管理和公共服务职能中的重要作用，最终实现促进社会管理创新、加快社会管理体制改革、构建社会主义和谐社会的目标。第三，国家要统筹规划、上下联动，从政策、规划、资金、人才等方面提供支持与服务，加强现代信息技术的建设。

4．研究新技术的应用带来的安全风险及应对策略

要加强研究以云计算、物联网、移动宽带为代表的新技术在电子政务信息资源共享建设的应用中所面临的新安全风险，并提出预防和应对方案。加强与研究机构、大学的合作，加大关键安全技术的研究和技术攻关力度。以技术研究为基础，多方论证，积极制定应对安全风险的相关策略。

5．加强新技术、新应用的自主可控

一是要鼓励国内企业积极申请专利，加强知识产权保护，提高自主专利的拥有数量与质量；同时要注重引进技术的消化吸收和再利用，围绕基础专利技术和引进的先进技术，及时、主动地形成更多的外围专利和自主知识产权。二是加强云计算、物联网中核心技术和关键设备的自主研发，加强信息技术产品供应链和信息技术外包服务的安全管理，大力支持信息技术产品的国产化，率先采购优质高效的本国产品和自主创新产品。

8.7 实施自主创新战略

1．加强研发，建立自主创新体系

依靠自主创新，推进我国电子政务重要信息系统装备、技术国产化，提高自主可控能力。加大力度支持事关国家信息安全的信息技术、产品的研发和产业化，实施信息安全技术研发、产业化重大专项，增加对信息安全保障关键技术研究的资金投入，形成拥有自主知识产权的信息安全技术和产品，在同等条件下优先使用自主创新产品、技术和服务。加强对云计算、物联网和宽带移动通信等新技术、新应用的跟踪研究，提高信息网络的自主可控能力。

2．健全电子政务信息资源共享的信任体系

加强对电子政务系统的用户身份管理，提高身份认证的互操作性水平；加强审计，提高责任追查认定能力；切实提高电子政务关键信息设施的安全保障能力，建设共享、融合、可信、安全的基础信息设施；按照《电子签名法》的要求推广新技术、新业务环境下的电子签名应用。

3．加强信息技术产品供应链管理

在我国信息技术产品自主可控能力明显不足、关键领域信息安全产品设备对国外供应商的依存度较高的条件下，加强信息技术产品供应链安全管理成为提升国家重要信息系统保障能力的重要手段。在产品研发生产、销售服务的各个环节，都要加强信息技术产品供应链的安全管理。第一，要加快供应链安全管理的制度建设，落实自主可控的安全策略，健全自主产权的保护政策；第二，要建立信息安全产品销售和采购的审查机制，可参照国际通用做法对境外产品采用可控策略；第三，规范信息产品的安全测评机制，鼓励合格的、国产化的信息产品在政府部门及其他关键领域的使用。

4．加强信息技术外包服务的安全管理

尽快制定政府部门信息技术服务外包安全管理办法，对关系国计民生的重要

行业、国防军工、科研院所开展信息安全管理体系认证、境外上市、利用外资、合作研究项目、信息技术产品捐赠、提供技术支持和外包服务等提出安全管理要求，保证重要信息系统的安全运行，确保重要敏感信息不泄露。对于信息技术外包服务，要定期开展信息安全等级评估工作，对评估不合格的服务提供商，要立即停止相关业务。加紧落实《关于加强信息安全管理体系认证安全管理的通知》，明确政府部门不得利用社会第三方认证机构开展信息安全管理体系认证，基础信息网络和重要信息系统运营单位如确需申请信息安全管理体系认证，应事先报行业主管或监管部门同意。

5．规范政府采购，提高自主可控能力

第一，要不断增强国家安全意识和国货意识。在可选择的情况下，各级政府部门应大力支持信息类产品的国产化，率先采购本国产品和自主创新产品，优先采用本土企业提供的信息技术服务，以有效保持和促进民族企业的发展和自主可控能力。第二，尽快明确“本国货物”的认定标准及量化指标。强制要求各部门在本国货物能够满足应用需求时，必须采购本国货物并优先采购自主创新产品；因技术原因确需采购非本国货物时，必须按照有关规定报相关部门审批，同时该产品也必须通过国家的信息安全检测认证，并以此为对价，要求国外厂商开放涉及信息产品的关键技术。建议在重要信息系统和政务业务关键部门的计算机、网络相关的设备采购中，制定限定国货的原则，并逐步将限定国货的原则全面推广至电子政务建设之中。

参考文献

[1] 钱学森．创建系统学（新世纪版）[M]．上海：上海交通大学出版社，2007.

[2] 钱学森．论系统工程（新世纪版）[M]．上海：上海交通大学出版社，2007.

[3] 钱学森，戴汝为．论信息空间的大成智慧[M]．上海：上海交通大学出版社，2007.

[4] 曲维枝．信息社会：概念、经验与选择（上、下册）[M]．北京：经济科学出版社，2005.

[5] 周宏仁．信息化论[M]．北京：人民出版社，2008.

[6] 乌家培．乌家培文库[M]．北京：中国计划出版社，2010.

[7] 刘鹤．中国电子政务发展的“四个需要”和“四个重点”[J]．电子政务，2004（4）：289-289.

[8] 杨学山．政府信息公开与电子政务建设[J]．电子政务，2008（7）：8-9.

[9] 钱学森，于景元，戴汝为．一个科学的新领域——开放的复杂巨系统及其方法论[J]．自然杂志，1990：526-532.

[10] 何德全．互联网时代信息安全的新思维[J]．科学中国人，2003（1）：14-15.

[11] 何德全．坚持“以人为本”的信息安全科学发展观[J]．信息安全与通信保密，2004（9）：1.

[12] 戴汝为，操龙兵．Internet——一个开放的复杂巨系统[M]．中国科学（E 辑），2003.

[13] 冯登国等著，蔡吉人审．信息安全体系结构[M]．北京：清华大学出版社，2008.

[14] 顾基发，唐锡晋．物理—事理－人理系统方法论：理论与应用[M]．上海：上海科技教育出版社，2006.

[15] 王新才．政府信息资源管理[M]．北京：科学出版社，2011.

[16] 何振．电子政务信息资源的共建与共享研究[M]．北京：中国社会科学出版社，2009.

[17] 徐晓，林杨锐．电子政务[M]．武汉：华中科技大学出版社，2009.
[18] 卢纹岱．SPSS for Windows 统计分析（第 2 版）[M]．北京：电子工业出版社，2002.
[19] 马国庆．管理统计：数据获取、统计原理、SPSS 工具与应用研究[M]．北京：科学出版社，2002.
[20] 王长胜．电子政务蓝皮书——中国电子政务发展报告 2009[M]．北京：社会科学文献出版社，2009.
[21] 王长胜．电子政务蓝皮书——中国电子政务发展报告 2010[M]．北京：社会科学文献出版社，2010.
[22] 洪毅，王长胜．电子政务蓝皮书——中国电子政务发展报告 2011[M]．北京：社会科学文献出版社，2011.
[23] 曼纽尔·卡斯特著．网络社会的崛起[M]．夏铸九译．北京：社会文献出版社，2006.
[24] 沈大风，周民．电子政务发展前沿（2011）[M]．北京：社会科学文献出版社，2011.
[25] 沈大风，周民．电子政务发展前沿（2014）[M]．北京：社会科学文献出版社，2014.
[26] 苏新宁，朱晓峰，吴鹏，等．政务信息资源管理与政府决策[M]．北京：科学出版社，2008.
[27] 赵战生，杜虹，吕述望．信息安全保密教程[M]．合肥：中国科学技术大学出版社，2006.
[28] 许国志．系统科学[M]．上海：上海科技教育出版社，2000.
[29] 哈肯著．协同学：大自然构成的奥秘[M]．凌复华译．上海：上海译文出版社，2001.
[30] 马费成，赖茂生．信息资源管理[M]．北京：高等教育出版社，2006.
[31] 汪向东，姜奇平．电子政务行政生态学[M]．北京：清华大学出版社，2007.
[32] 严进．信任与合作——决策与行动的视角[M]．北京：航空工业出版社，2007.
[33] 王越，罗森林．信息系统与安全对抗理论[M]．北京：北京理工大学出版社，2006.
[34] 张来武，孙志海．世界前沿技术发展报告 2010[M]．北京：科学出版社，2011.

[35] 胡小明．广州市电子政务信息共享步入良性循环的原因分析[J]．电子政务，2008：58-66.

[36] 宁家骏．电子政务工程实务概论[M]．北京：中国市场出版社，2006.

[37] 普里戈金著．从存在到演化[M]．曾庆宏，严士健，马本堃，等译．北京：北京大学出版社，2007.

[38] 靖继鹏，张向先，李北伟．信息经济学[M]．北京：科学出版社，2007.

[39] 冯惠玲．政府信息资源管理[M]．北京：中国人民大学出版社，2006.

[40] （德）乌尔里希贝克 Ulrich Beck，何博闻．风险社会[M]．上海：译林出版社，2009.

[41] Fioravanti F., Nardelli E.,Identity management for e-government servics[J].Digital Government.Springer, 2007:331-352.

[42] Akbulut, A. Y..An Investigation of the Factors that Influence Electronic Information Sharing Between State and Local Agencies., Louisiana State University, 2003.

[43] Akhilesh, B., & Sudha. IAIS: A Methodology to Enable Interagency Information sharing in E-Government[J]. Journal of Database Management, 2003, Vol. 14(4): 59-80.

[44] Barua, A., & Ravindran, S. Reengineering Information Sharing Behavior in Organization. Journal of Information Technology, Vol. 11(3):261-272.

[45] Bekkers, V. Flexible Information Infrastructures in Dutch E-Government Collaboration Arrangements:Experiences and Policy Implications[J]. Government Information Quarterly, 2009, Vol. 26:60-80.

[46] Beldad, A., Jong, M.D., Steehouder, M. I Trust not Therefore it Must be Risky: Determinants of the Perceived Risks of Disclosing Personal Data for E-Government Transactions[J]. Computers in Human Behavior, 2011, Vol. 27(6): 2233-2242.

[47] Dawes, S. S. Interagency information sharing: Expected benefits, manageable risks[J]. Journal of Policy Analysis and Management, 1996, Vol. 15(3):377-394.

[48] Drake, D. B., Steekler, N. A., & Koch, M. J. Information Sharing in and Across Government Agencies: The Role and Influence of Scientist, Politician, and Bureaucrat Subcultures. Social Science Computer Review,2004, Vol. 22(1):67-84.

[49] Evgeniou, T., & Cartwright, P. Barriers to Information Management. European Management Journal, 2005, Vol. 23(3):293-299.

[50] Gil-Garcia, J. R. N., & Pardo, T. A. E-government success factors: Mapping practical tools to theoretical foundations[J]. Government Information Quarterly, 2005, Vol. 22(2):187-216.

[51] Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. Collaborative e-Government: Impediments and benefits of information-sharing projects in the public sector[J]. European Journal of Information Systems, 2007, Vol.16(2): 121-133.

[52] Grover, V. An Empirically Derived Model for the Adoption of Customer-Based Interorganizational Systems[J]. Decision Sciences, 1993, Vol. 24(3):603-640.

[53] Kent, A. The Goals of Resource Sharing in Libraries. Paper presented at the 1976 Conference on Resource Sharing in Libraries, 1977.

[54] Kolekofski Jr, K. E., & Heminger, A. R. Beliefs and Attitudes Affecting Intentions to Share Information in an Organizational Setting[J]. Information＆Management，2003, Vol. 40(6):521-532.

[55] Kwon, H., Pardo, T. A., Burke, G. B. Interorganizational Collaboration and Community Building for the Preservation of State Government Digital Information: Lessons from NDIIPP State Partnership Initiative[J]. Government Information Quarterly, 2009, Vol. 26:186-192.

[56] Lambrinoudakis, C. Security requirements for E-government services: A methodological approach for developing a common PKI-based security policy[J]. Computer Communications, 2003, Vol. 26(15):1873-1883.

[57] Landsbergen, D., & Wolken, G. Government Information Systems and the Fourth Generation of Information Technology[J]. Public Administration Review, 2001, Vol.61(2):206-218.

[58] Landsbergen, D., & Wolken, G. Realizing the Promise: Government Information Systems and the Fourth Generation of Information Technology[J].Public Administration Review, 2002, Vol. 61(2):206-220.

[59] Roberts, A. S., & Governance, N. Networked Governance, Information Sharing and the Threat to Government Accountability. Government Information Quarterly, 2004, Vol.21(3):249-267.

[60] Rosenthal, A., Mork, P., Li, M.H, et al. Cloud Computing: A New Business Paradigm for Biomedical Information Sharing[J]. Journal of Biomedical Information, 2010, Vol. 43:342-353.

[61] Shin, S. K., Ishma, M., & Sanders, G. L. An empirical investigation of socio-cultural factors of information sharing in China. Information & Management, 2007, Vol.44(2):165-174.

[62] Valdés, G., Solar, M., Astudillo, H., et al. Conception Development and Implementation of an E-Government Maturity Model in Public Agencies[J]. Government Information Quarterly, 2011, Vol. 28:176-187.

[63] Yang, T., Maxwell, T. A. Information-Sharing in Public Organizations: A Literature Review of Interpersonal Intra-Organizational and Inter-Organizational Success Factors[J]. Government Information Quarterly, 2011, Vol. 28:164-175.

[64] Zaheer, A., McEvily, B., & Perrone, V. Does Trust Matter? Exploring the Effects of Interorganizational and Interpersonal Trust on Performance[J]. Organization Science, 1998, Vol. 9(2):141-159.

[65] K. Layne, J Lee. Developing fully functional E-government: A four stage model[J]. Government Information Quarterly, 2001, Vol. 18(2):122-136.

[66] MR Benioff, ED Larowska. Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005.3.

[67] I Chopin, J Niessen. Commission of the European Communities, Europe 2020: Commission proposes new economic strategy in Europe. 2010.3.

[68] Alexander Schellong, Philipp Girrger.An Analysis of eParticipation and Web 2.0 Applications of Germany’s 50 largest Cities and 16 Federal States[R].Public Sector Study Series, 2010.6.

[69] D.Bell, L.Padula. Security Computing Systems: Mathematical Foundation and Model. MITRE Report, Bedbord, MA, 1975.

[70] D.Bell, L.Padula. Security Computing Systems: Unified Exposition and Multics Interpretation. Technical Report MITRE-2997 Rev.1, Bedbord, MA, 1975.

[71] K. Biba. Integrity Considerations for Secure Computer Systems. Technical Report MITRE 3153 Vol.I, MITRE Corporation, Bedbord, MA, 1977.

[72] S.B. Lipner. Non-Discretionary Controls for Commercial Applications. Pro. 1982 Sympsium on Privacy and Security, 1982:2-10.

[73] S.B. Lipner. A Comparison of Commercial and Military Computer Security Policies. Proc. of the 1987 IEEE Symposium on Security and Privacy, 1987.

[74] D.D. Clark, D.R. Wilson. Non Discretionary Controls Commercial Applications. Proc. of the IEEE Symposium on Security and Privacy, 1997:184-194.

[75] F.C.B. David, N. Michael. The Chinese wall Security Policy. IEEE Symposium on Research in Security and Privacy, 1989:206-214.

[76] National Security Agency. National Information Systems Security Glossary. NSTISSI 4009 Fort Meade, MD.2000.9.

[77] J. McCumber. Information Systems Security: A Comprehensive Model. Prco. Of the 14th National Computer Security Conference. NIST. Baltimore, MD. 1991.10.

[78] W.V.Maconachy, C.D.Schou. A model for information assurance: an integrated approach. Proceedings of the 2001 IEEE Workshop on Information Assurance Security. NY, 2001:180-185.

[79] Information Assurance Technical Framework 3.1, National Security Agency Information Assurance Solutions Technical Directors, 2002.9.

[80] M.Bishop, Computer Security: Art and Science. Addison-Wesley Press, 2002.

[81] Federal Office for Information Security .IT Baseline Protection: the Basis for IT Security. BSI publications, 2006.

[82] Bertino E., Squicciarini A.C., Bhargav-Spantzel A. Trust Negotiation in Identity Management[J]. IEEE Security&Privacy, 2007, Vol. 5(2):55-63.

[83] Sarah Waheed Sher, Division for Public Administration and Development Management, United States. UN Global E-government Readiness Report 2005 From E-government to E-inclusion[R].New York:United Nations, 2005.

[84] Daniel S.Soper, Haluk Demirkan, Micheal Goul. An interorganizational knowledge-sharing security model with breach propagation detection. Inf Syst Front, 2007, Vol. 9(9):469-479.

[85] Douglas Harris, Latifur Khan, Raymond Paul, et al. Standards for secure data sharing across organizations[J]. Computer Standard & Interfaces, 2007, Vol. 29(1): 86-96.

[86] P. Liu, C. Amit. Trust-Based Secure Information Sharing Between Federal Government Agencies[J].Journal of the American Society for Information Science and Technology, 2005, Vol. 56(3):283-298.

[87] Lambrinoudakis, C. Security Requirements for E-Government Services: A Methodological Approach for Developing a Common PKI-Based Security Policy[J]. Computer Communications, 2003, Vol. 26(16):1873-1883.

[88] Sang M.Lee， Xin Tan， Silvana Trimi. Current Practices of Leading e-Government Countries[J].Communication of the ACM, 2005, Vol. 48(10):99-104.

[89] Office of Management and Budget. Implementing the President's management agenda for e-government[R]，2003.

[90] 沈昌祥，张焕国，冯登国，等．信息安全综述[J]．中国科学（E 辑），2007，37（2）：129-150.

[91] 曲成义．电子政务安全体系框架[J]．计算机安全，2002（3）：19-20.

[92] 崔书昆．我国信息安全今后工作刍议[J]．金融电子化，2010（12）：27.

[93] 赵国俊．浅议我国信息资源开发利用战略思想的形成与发展．档案学通讯，2009（3）：4-6.

[94] 冯登国，张敏，张妍，等．云技术安全研究．软件学报，2011，22（1）：72-83.

[95] 吕欣. 电子政务信息安全保障体系研究[R]. 国家信息中心博士后研究报告，2008.

[96] 吕欣. 电子政务信息资源共享中信任机制的构建[J]. 信息网络安全，2003（3）：11-13.

[97] 董海欣．电子政务环境下政府信息资源共享模式与运行机制研究[D]．吉林大学，2008.

[98] 范静．G2G 电子政务信息共享及信息安全实证研究[D]．上海交通大学，2008.

[99] 孟薇．电子政务信息安全研究[D]．天津大学，2007.

[100] 张进京译．德国联邦经济与劳工部 德国联邦教育研究部，2006 年德国信息社会行动纲领——德国走向信息社会的主体计划[J]. 信息化参考，2005（10）.
[101] 小林麻理著．IT 的发展与个人信息保护[M]．夏平，王俊红，周伟民译．北京：经济日报出版社，2007.
[102] 李守鹏．信息安全及其模型与评估的几点新思路[D]．四川大学，2002.
[103] 国家质量监督检验检疫总局．GB/T 24294—2009 信息安全技术基于互联网电子政务信息安全实施指南[S]．北京：中国标准出版社，2009.
[104] 郭杰．对修订我国《保密法》的几点思考[J]．信息网络安全，2008（3）：1.
[105] 方滨兴，殷丽华．关于信息安全定义的研究[J]．信息网络安全，2008（1）：8-10.
[106] 杨飞．对“十二五”电子政务工作的若干思考[J]．电子政务，2011（11）：85-89.
[107] 查先进．网络环境下政府信息资源的共享与保密[J]．图书情报知识，2002（4）：2-5.
[108] 何振，周伟．电子政务信息资源共建共享的经济特性及其效率分析[J]．情报杂志，2005（4）：10-13.
[109] 完颜绍华，杨华军，许庆瑞．组织创新的整合观[J]．自然辩证法研究，2001（1）：33-36.
[110] 雷婷．欧盟多层治理对其电子政务建设的影响[D]．北京：中国社会科学院研究院，2010.
[111] 张海燕．借鉴美日欧电子政务建设经验的思考[J]．情报探索，2011（8）：78-79.
[112] 曹学勤，郭利．电子政务以欧洲一体化的名义进行[J]．上海信息化，2010（8）：82-86.
[113] 朱根．信息服务创新推进日本电子政务变革[J]．情报资料工作，2010（4）：76-79.
[114] 斯东咏．中央领导地方——看加拿大联邦政府如何引领国家电子政务建设[J]．科技信息，2011（21）：475-484.
[115] 孙立立．美国信息安全战略综述[J]．信息网络安全，2009（8）：7-10.
[116] 国家信息技术安全研究中心．俄罗斯信息安全建设研究[J]．信息网络安全，2009（8）：37-39.
[117] 国家信息安全研究中心．欧盟信息安全建设研究[J]．信息网络安全，2009（8）：31-32.
[118] 汪向东．关于我国电子政务领导体制的思考[J]．中国信息界，2009（7）：14-17.

[119] 李柯．日本行政机关网络信息安全对策体制[J]．国土资源信息化，2007（6）：31-35.
[120] 杨国辉．世界各国信息按照政策与策略[J]．中国信息安全，2010（11）：16-17.
[121] 李理．美日信息社会建设与发展的比较研究[D]．东北财经大学，2009.
[122] 华云．欧盟电子政务动态[J]．信息化建设，2010（2）：39-41.
[123] 陶世明．建立健全监控体系，保三网融合安全[J]．中国信息安全，2010（9）：37-38.
[124] 赵一荣．大数据时代电子政务信息资源共享策略研究[J]．大众科技，2015（17）：162-163.
[125] 武青海，夏洪波．大数据时代下政府部门信息资源共享策略研究[J]．统计与管理，2015（11）：104-105.
[126] 孙一冰，卓俊，刘嘉怡．大数据与电子政务[J]．中国税务，2014（12）：40-41.

反侵权盗版声明